Systemhandbuch

Das Sicherheitsprogramm für die Industrien der Welt

safety INTEGRATED

5. Auflage

SIEMENS

„Das Verhüten von Unfällen darf
nicht als eine Vorschrift des
Gesetzes aufgefasst werden,
sondern als ein Gebot
menschlicher Verpflichtung
und wirtschaftlicher Vernunft.“

Werner von Siemens,
Berlin im Jahr 1880

Inhalt

1 Vorschriften und Normen

1.1 Allgemeines 1/2
1.2 Vorschriften und Normen in der Europäischen Union (EU) 1/3
Grundprinzipien der gesetzlichen Anforderungen in Europa 1/3
Arbeitsschutz in der EU 1/4
Maschinensicherheit in Europa 1/5
Prozesstechnik in Europa 1/20
Feuerungsanlagen in Europa 1/25
1.3 Gesetzliche Anforderungen und Standards zur Sicherheit am Arbeitsplatz in Nordamerika 1/26
USA allgemein 1/26
Maschinensicherheit 1/27
Prozessindustrie in USA 1/30
Arbeitsschutzbestimmungen und Sicherheitsnormen in Kanada 1/31
1.4 Sicherheitsanforderungen für Maschinen in Japan 1/34
1.5 Wichtige Adressen 1/35

2 Spezifikation und Design sicherheitsrelevanter Steuerungen für Maschinen

2.1 Überblick 2/2
2.2 Entwurfs- und Realisierungsprozess der Maschine, Risikobeurteilung, Prozess der Risikominderung 2/3
2.3 Hängt die Schutzmaßnahme von einer Steuerung ab? 2/9
2.4 Spezifikation der Sicherheitsanforderungen 2/14
2.5 Entwurf und Realisierung der (sicherheitsrelevanten) Steuerung nach IEC 62061 2/15
Philosophie/Theorie 2/17
Systemdesign für eine Sicherheitsfunktion 2/23
2.6 Entwurf und Realisierung der sicherheitsbezogenen Teile einer Steuerung nach EN 954-1 (ISO 13849-1 (rev)) 2/34

3 Sensor- / Aktor Einbindung

3.1 Überblick 3/2
3.2 Merkmale 3/3
3.3 Normen im Überblick 3/4
3.4 Sensor/Aktor Anbindung 3/6
Konventionelle Sensoreinbindung ohne sicherheitsgerichtete Kommunikation über Feldbusse 3/12
Sensor/Aktor Anbindung ohne sicherheitsgerichtete Kommunikation 3/13
Anbindung am AS-Interface mit ASIsafe 3/19
Sensor Anbindung am AS-Interface mit ASIsafe 3/20
Aktor Anbindung am AS-Interface mit ASIsafe 3/22
Anbindung am PROFIBUS mit PROFIsafe 3/24
Sensor Anbindung am PROFIBUS mit PROFIsafe 3/25
Sensor Anbindung an fehlersichere SIMATIC Eingabebaugruppen/Module 3/25
Aktor Anbindung am PROFIBUS mit PROFIsafe 3/32

4 Fehlersichere Steuerungen über Standard-Feldbusse

4.1 PROFIsafe 4/2
Merkmale / Nutzen 4/3
Einsatzbereich von PROFIsafe 4/4
Die PROFIsafe-fähigen Produkte 4/4
PROFIsafe im 7-Schichten-Kommunikationsmodell 4/4
PROFIsafe-Funktionen 4/5
PROFIsafe im Zusammenspiel mit TIA 4/7
4.2 ASIsafe 4/7
Übersicht 4/7
Kundennutzen 4/8
Highlights 4/9
Anwendungsbereich 4/9
Prinzipieller Aufbau und Funktion 4/9
Integration in TIA 4/14

5 Sicherheitsgerichtete Schalttechnik

5.1 SIRIUS Positionsschalter 5/2
5.2 SIRIUS Not-Halt 5/7
5.3 SIRIUS Befehls- und Meldegeräte 5/8
5.4 SIRIUS Sicherheitsschaltgeräte 5/11
Übersicht 5/11
Merkmale 5/11
Anwendungsbereich 5/11
Produktfamilie/Produktgruppen 5/12
Aufbau 5/13
Funktionen 5/13
Integration 5/15
Beispiele 5/16
Technische Daten 5/18
5.5 ASIsafe 5/20
Produktfamilie/Produktgruppen 5/20
Technische Daten 5/22
Beispiel Verpackungsmaschine 5/23
5.6 ET 200S Safety Motorstarter Solution 5/24
Übersicht 5/24
Anwendungsbereich 5/24
Merkmale 5/25
ET 200S Motorstarter Solution Local 5/26
ET 200S Motorstarter Solution PROFIsafe 5/30
Aufbau 5/37
Technische Daten 5/38

6 Fehlersichere optische Sensoren

6.1 SIGUARD Laserscanner LS4 6/2
Übersicht 6/2
Anwendungsbereiche des SIGUARD Laserscanners LS4 6/3
Produktfamilien/Produktgruppen 6/4
Aufbau 6/5
Funktionen 6/6
Systemeinbindung 6/7
Anwendungshinweise 6/8
Schutzfeldberechnung 6/9
Technische Daten 6/12
6.2 SIGUARD Lichtvorhänge und Lichtgitter 6/14
Übersicht 6/14
Merkmale 6/14
Anwendungsbereich 6/16
Funktionen 6/21
6.3 SIGUARD Lichtschranken 6/28
6.4 SIGUARD Schaltleisten 6/32

7 Fehlersichere Steuerungen

7.1 Übersicht 7/2
7.2 Merkmale 7/3
7.3 Anwendungsbereich 7/5
7.4 Produktgruppe/Produktfamilie 7/6
7.5 Engineering 7/10
7.6 Aufbau 7/11
7.7 Funktionen 7/12
7.8 Beispiele 7/14
7.9 Technische Daten 7/18

8 Fehlersichere Motion Control Systeme

8.1 SINUMERIK Safety Integrated - Das Sicherheitspaket für Bearbeitungsmaschinen 8/2
Kurzbeschreibung 8/3
Ausrüstungskomponenten 8/5
Systemvoraussetzungen 8/8
Sicheres Stillsetzen 8/9
Überwachung von Geschwindigkeit und Position 8/13
Verknüpfung sicherheitsgerichteter Prozess-Signale 8/14
Absturzsicherung bei Vertikalachsen 8/15
Integriertes und teilautomatisiertes Abnahmeprotokoll 8/19
Zwangsdynamisierung bei SINUMERIK Safety Integrated 8/21
Sensor-/Aktor-Einbindung – Grundlagen 8/22
Sensor-/Aktor-Einbindung über getrennte Hardware E/A von PLC und NC 8/24
Sensor-/Aktor-Einbindung über die fehlersicheren Baugruppen von ET 200S PROFIsafe 8/30
Anwendungsbeispiele 8/31
Zertifizierung 8/31
8.2 Safety Unit 8/32
8.3 Safety Integrated für Motion Control Systeme 8/34

9 Fehlersichere Antriebe

9.1 MASTERDRIVES und SIMODRIVE 611universal 9/2
9.2 SINAMICS Safety Integrated 9/4
9.3 Frequenzumrichter SIMATIC ET 200S FC
Übersicht 9/6
Nutzen 9/7
Anwendungsbereich 9/7
Aufbau 9/8
Funktionen 9/8
Integration 9/10
Technische Daten 9/12

10 Referenzen

10.1 Fehlersichere SIMATIC Controller im Rohbau von Opel Belgien 10/2
10.2 Sicherheitstechnik bei Toyota Kanada 10/4
10.3 Karosseriebau mit dezentraler Sicherheit bei Ford Australien 10/6
10.4 SPS-basiertes Sicherheitskonzept in der LKW-Räderfertigung bei Michelin Deutschland 10/9
10.5 Wilde Fahrt bei Madame Tussauds 10/12
10.6 Saatgutaufbereitung – Steuerung einer Pumpenanlage für Chemikalien mit ASIsafe 10/14
10.7 AS-Interface vereinfacht Arbeitsschutz bei UPS 10/16
10.8 CROWN Vourles – Verpackungsindustrie sicher mit Safety Motorstarter Solution PROFIsafe 10/19
10.9 Mehr Sicherheit in der Automobilindustrie 10/22
10.10 Neuer Standard für Werkzeugmaschinen 10/23
10.11 Sicherheit bei der Produktprüfung von Arbeitsschutztechnik 10/25
10.12 Sicherheit und Taktgefühl 10/30
10.13 Sicherer Halt in der Druckindustrie 10/32

11 Anhang

11.1 Begriffe und Abkürzungen 11/2
11.2 Literatur 11/6
11.3 Kontakt – Internet und Hotline 11/6
11.4 Seminarangebot – Sicherheitstechnik, Normen und Richtlinien 11/7
11.5 Stichwortverzeichnis 11/15

Vorwort

Vorschriften und Normen 1

Spezifikation und Design sicherheitsrelevanter Steuerungen für Maschinen 2

Sensor-/Aktoreinbindung 3

Fehlersichere Kommunikation über Standard-Feldbusse 4

Sicherheitsgerichtete Schalttechnik 5

Fehlersichere optische Sensoren 6

Fehlersichere Steuerungen 7

Fehlersichere Motion Control Systeme 8

Fehlersichere Antriebe 9

Referenzen 10

Anhang 11

Liebe Leserinnen und Leser,

Helmut Gierse
A&D Bereichsvorstand

Applikationen im Bereich der Maschinensicherheit oder Prozesstechnik – moderne Technologien im Automatisierungsprozess erfordern ein Höchstmaß an Sicherheit für Mensch, Maschine und Umwelt.

Das bereits mehrfach aktualisierte Systemhandbuch „Safety Integrated" zeigt, wie Gefahren, die durch Funktionsfehler verursacht werden, vermindert oder beseitigt werden können.

Von der Sensorik über die Auswerteeinrichtungen bis hin zur sicheren Ausführung bietet „Safety Integrated" mit den Produktgruppen SIRIUS, SIGUARD, SIMATIC, und SINUMERIK/ SIMODRIVE maximalen Schutz vor Funktionsfehlern.

Diese Produktgruppen haben sich bereits jahrelang im weltweiten Einsatz in der Standard-Automation bewährt. Seit der Zulassung der sicherheitsgerichteten Kommunikation über PROFIBUS und über das Aktor-Sensor-Interface – ASIsafe können diese Komponenten auch im System kombiniert werden.

Neben der konventionellen Verdrahtung zwischen den Einzelkomponenten entsteht additiv durch den Einsatz von Standard-Feldbussystemen auch für die Sicherheitstechnik eine Systemdurchgängigkeit, die ein wirtschaftlicheres Engineering ermöglicht, den Hardware-Aufwand aufgrund der Verwendung gemeinsamer Komponenten verringert und gleichzeitig auch die Anlagenverfügbarkeit über eine bessere Diagnosefähigkeit erhöht.

Offen und durchgängig

Eine Automatisierungsanlage besteht hauptsächlich aus Standardkomponenten wie Standard-SPS, Antrieben usw.

Der Anteil der Sicherheitstechnik einer Gesamtanlage kann je nach Einsatzbereich unterschiedlich hoch sein. Unabhängig von dem Einsatzbereich besteht die Sicherheitsebene jedoch immer aus einer Kette von Sensoren, Auswertegeräten und Aktoren für einen sicheren Zustand der Anlage oder Maschinen. In vielen Applikationen sind jedoch die beiden Ebenen, Standard- und Sicherheitstechnik einer Anlage, immer noch strikt voneinander getrennt. In der Regel werden unterschiedliche Engineering-Methoden und -Werkzeuge angewendet, was einen größeren Aufwand bei der Ausbildung des Personals notwendig macht und beide Ebenen müssen aufwendig miteinander verdrahtet werden.

Die Forderungen nach Einsparungspotenzial können vor allem durch die Wahl der richtigen Installationstechnik erfüllt werden. In der Standardtechnik führte die konsequente Umsetzung der Dezentralisierung mit der Nutzung von modernen Feldbustechnologien bereits zu erheblichen Kosteneinsparungen. Weitere Einsparmöglichkeiten ergeben sich daher durch die zusätzliche Übertragung der sicherheitsrelevanten Signale über diese bereits verlegten Standard-Feldbusse.

„Safety Integrated“ ist die konsequente Umsetzung dieses Konzepts.
Mit diesem Konzept wachsen sowohl die Standard- als auch alle Sicherheitskomponenten zu einem einheitlichen, transparenten wirtschaftlichen Gesamtsystem zusammen.

Aufwändige Verdrahtungen für Diagnose und Rückmeldungen können entfallen. Einheitliche Engineering-Werkzeuge und -Methoden sowie Visualisierungskonzepte sorgen bei Safety Integrated für Einsparungen sowohl bei der Planung als auch der Installation und der Wartung.

Veränderungen in der Normenlandschaft führen dazu, dass Konstrukteure bei der Planung von sicherheitsrelevanten Maschinen- und Anlagensteuerungen Ihre Methodik anpassen müssen.

Dies unterstützen wir durch leicht verständliche Unterlagen und Workshops für den Gebrauch, wie auch die Auslegung dieser Normen.

Durch den regen Austausch mit Anwendern werden benötigte Elemente nach und nach definiert und entwickelt, so dass auch in den nächsten Jahren weitere Produkte die Palette noch runder machen werden.

Trends in der Automatisierungstechnik, die bereits die heutige Automatisierungswelt beeinflussen, werden selbstverständlich auch bald in Safety Integrated zu finden sein. Als Beispiel sei das kommende Kommunikationsprotokoll PROFINET safety oder die drahtlose Kommunikation genannt. Ferner werden auch Trends durch Safety Integrated initiiert. Durch die verbundene Vorbildfunktion werden Maßstäbe in Beratung sowohl bei qualitativen oder quantitativen Nachweisen gesetzt, und durch den begeisterten Anwender menschliche Verpflichtung und wirtschaftliche Vernunft vereint.

Gemeinsam mit unseren Kunden die Kompetenz für funktionale Sicherheit auszubauen ist unsere Mission!

Ihr

Helmut Gierse

Heinz Gall

Leiter des Geschäftsfeldes
Automation, Software und
Informationstechnologie (ASI)
TÜV Industrie Service GmbH, Köln
TÜV Rheinland Group

In vielen unterschiedlichen Anwendungsbereichen (Maschinen- und Fördertechnik, Prozessindustrie, Gebäudetechnik etc.) werden Systemen und Komponenten der Automatisierungstechnik sicherheitsrelevante Aufgaben übertragen. Das bedeutet, dass das Leben und die Gesundheit von Personen sowie die Unversehrtheit von Anlagengütern und der Umwelt von der ordnungsgemäßen Funktion der Systeme und Komponenten abhängt.

Heute wird die ordnungsgemäße Funktion von Systemen und Komponenten unter dem Begriff „Funktionale Sicherheit / Functional Safety" international behandelt. Dies wird insbesondere durch den im Frühjahr 2000 verabschiedeten Standard IEC 61508 „Funktionale Sicherheit von elektrischen, elektronischen und programmierbaren elektronischen sicherheitsgerichteten Systemen" dokumentiert. Mittlerweile ist der Standard auch als EN 61508 und DIN EN 61508 / VDE 0803 erschienen.

Dieser Standard gilt als anwendungsunabhängiger Basisstandard und wendet sich an die Entwickler anwendungsspezifischer Standards, sowie inhaltlich (Beschreibung von Maßnahmen zum Sicherheitskonzept, fehlervermeidende und fehlerbeherrschende Maßnahmen für Hard- und Software) im wesentlichen an die Hersteller sicherheitsgerichteter Systeme und Komponenten.

Von den anwendungsorientierten Normungskreisen wurde dies schon aufgenommen. Die ersten Beispiele sind die IEC 61511 für die Prozessindustrie und EN 50156 für die elektrische Ausrüstung von Feuerungsanlagen. Im Bereich der Sicherheit von Maschinen ist die IEC 62061 für sicherheitsrelevante Steuerungssysteme von Maschinen zu erwarten. Im Bereich der Maschinensicherheit sind selbstverständlich auch die anwendungsspezifischen Standards wie z.B. die EN 954 zu berücksichtigen. Für diesen Standard gibt es auch Aktivitäten um die Betrachtungsweisen der IEC 61508 in Bezug auf z.B. quantitative Größen zu integrieren. Im Bereich der Gebäudeautomation ist ein VDMA Einheitsblatt 24200-1 erschienen, das ebenfalls die Betrachtungsweise der IEC 61508 berücksichtigt.

Für die Zukunft ist somit zu erwarten, dass weitere Anwendergremien den vorliegenden Basisstandard für ihre Arbeit verwenden, um die Anforderungen an sicherheitsgerichtete Systeme und Komponenten zu vereinheitlichen. Dies macht insbesondere deshalb Sinn, weil die Prinzipien der Risikobetrachtung, Risikoreduzierung und der sicherheitsgerichteten Funktion auf unterschiedlichste Anwendungsbereiche übertragen werden können. Aus Sicht der Anwendung wären dann nur noch wenige Aspekte wie z.B. geforderte Reaktionszeiten oder der sichere Zustand für den jeweiligen Prozess zu betrachten.

Den Herstellern wird dadurch ermöglicht, Systeme und Komponenten zu entwickeln, die in unterschiedlichen Anwendungsbereichen für Sicherheitsaufgaben mit vergleichbarem Risiko eingesetzt werden können. Dazu müssen die folgenden allgemein gültigen Angaben zu den jeweiligen Komponenten zur Verfügung stehen:

- Maximal erreichbarer Safety Integrity Level
- Hardware Fehlertoleranz in Verbindung mit dem Anteil der sicheren Ausfälle (Summe der Ausfälle in sicherer Richtung plus Summe der durch interne Diagnose erkannten und beherrschten Ausfälle) bezogen auf die Summe der gesamten Ausfälle
- Gefährliche Versagenswahrscheinlichkeit
- Hinweise zur Anwenderprogrammierung, Konfiguration und Betrieb

Die genannten Kriterien erlauben dann in der Anwendung übergreifend auch die Betrachtung von sicherheitsgerichteten Funktionen, die ja in der Regel aus Sensorik, Logik (z.B. SPS) und Aktorik, sowie der Kommunikation zwischen diesen Komponenten bestehen.

Da die Feldgeräte, Sensorik und Aktorik, sich durch immer mehr „Intelligenz" auszeichnen, wird auch die sichere Kommunikation zwischen den Komponenten einer sicherheitsgerichteten Funktion vermehrt über Bussysteme erfolgen.

Im Bereich der standardisierten, sicherheitsgerichteten Bussysteme wurde innerhalb der letzten Jahre ein erheblicher Fortschritt erzielt.

Dieser Fortschritt besteht einerseits aus der Entwicklung eines Grundsatzes für die „Prüfung und Zertifizierung von Bussystemen für die Übertragung sicherheitsrelevanter Nachrichten" und andererseits wurden Konzeptprüfungen solcher Bussysteme erfolgreich abgeschlossen.

Mittlerweile sind auch sicherheitsgerichtete Geräte / Komponenten zum Betrieb an diesen Bussystemen auf dem Markt verfügbar. Damit können Geräte unterschiedlicher Hersteller an standardisierten sicheren Bussystemen betrieben werden.

Hier sind die Hersteller aufgefordert, weitere Geräte für diese Bussysteme zu entwickeln.

Die TÜV Rheinland Group, insbesondere mit dem Geschäftsfeld Automation, Software und Informationstechnologie, unterstützt dabei weltweit (Europa, USA, Japan) Hersteller, Projekteure und Anwender bei der Umsetzung der oben genannten sicherheitstechnischen Aufgaben.

Systeme und Komponenten werden nach erfolgreicher Prüfung zertifiziert und erhalten das FS–Prüfzeichen „Funktionale Sicherheit" um die Übereinstimmung mit den Anforderungen der Normen und Standards zu dokumentieren. Weiterhin werden Managementsysteme zur funktionalen Sicherheit „FSM" bezogen auf den Lebenszyklus der Komponenten / Systeme und Experten / Ingenieure der Funktionalen Sicherheit „FS Exp/ FS Eng" qualifiziert und zertifiziert.

Projekteure und Anwender werden unterstützt um die funktionale Sicherheit auch für die Anwendung und die implementierten Sicherheitsfunktion zu erreichen.

Köln, den 2. September 2004

Alfred Beer

Management
Automation, Software and
Electronics IQSE
TÜV Automotive GmbH,
TÜV SÜD Gruppe, München

Systemzertifizierung

Die SIMATIC S7 Distributed Safety ist als sicherheitsgerichtetes programmierbares System durch den TÜV SÜD zertifiziert. Es ist somit geeignet für den Einsatz in sicherheitsgerichteten Anwendungen mit einem hohen potenziellen Gefährdungsrisiko, z.B. Fertigungstechnik, Maschinenbau, Prozesstechnik und Offshore Prozessen.

Zertifizierung durch den TÜV SÜD

Die Prüfung und Zertifizierung durch den TÜV SÜD als unabhängigen und akkreditierten Dritten bringt erhebliche Vorteile mit sich wie

- klare Positionierung des Produkts im internationalen Wettbewerb als ein durch eine weltweit führende Prüfstelle zertifiziertes qualitativ hochwertiges System
- hohe Zukunftssicherheit beim Festlegen der Prüfgrundlagen
- Prüfung unabhängig von internen Firmeninteressen
- hohe Akzeptanz im Markt
- problemlose Anerkennung der Zertifizierung weltweit.

Vorteile der Zertifizierung für den Endanwender

Bei Beachtung der Projektierungsrichtlinien muss sich der Endanwender keine weiteren Gedanken über die Funktionale Sicherheit machen. Die Steuerung verfügt über eine „eingebaute" anerkannte Funktionale Sicherheit.

Etwaige Abnahmebehörden müssen daher nur den korrekten Einsatz und die Einhaltung der Projektierungsrichtlinien begutachten.

Dabei dient die vorhandene Zertifizierung als Basis und muss nicht weiter hinterfragt werden.

Vorgehensweise bei der Zertifizierung

Grundsätzlich war die Zertifizierung an der IEC 61508 ausgerichtet. Zudem wurde auch die DIN V VDE 0801 herangezogen. Daher kamen deterministische als auch probabilistische Fehlermodelle zur Anwendung.

Aufgrund der Architektur der Verarbeitungseinheit ist eine hochwertige Fehlererkennung und Fehlerbeherrschung notwendig.

Der Nachweis dieser hohen Fehleraufdeckungsrate war nicht nur für die Siemens AG eine Herausforderung, sondern auch die Bewertung seitens des TÜV SÜD. Durch die enge Zusammenarbeit und Einbindung in den kompletten Entwicklungsprozess wurde der TÜV SÜD in die Lage versetzt, sich ein eigenes detailliertes Bild über das System und die dargelegten Argumente zu machen. Die Erfahrung und das Know How des TÜV SÜD wurde bei vielen innovativen Ansätzen immer wieder gefordert, um letztendlich mit dem System auf dem Weg der IEC 61508 zu bleiben.

Eine weitere Anforderung ist das Management der Funktionalen Sicherheit gemäß IEC 61508. Auch hierbei ist der TÜV SÜD von Anfang an mit in den Prozess als Begutachter eingebunden worden.

Zusätzlich wurde von Anfang an die Zertifizierung gemäß relevanter UL Standards angestrebt. Dazu wurde UL eng mit in die Zertifizierung durch TÜV SÜD eingebunden. Dadurch konnten zeitaufwendige und kostenintensive Doppelaktivitäten vermieden werden.

Basis der Zertifizierung

Im Rahmen einer erfolgreichen Zertifizierung sind mehrere Teilbereiche zu betrachten. Diese umfassen nicht nur die Funktionale Sicherheit, sondern auch Aspekte wie Primäre Sicherheit, Elektromagnetische Verträglichkeit und auch Anforderungen hinsichtlich Applikationen. Erst bei Erfüllung aller Anforderungen aus den Teilbereichen steht ein für den Anwender sicheres und verfügbares System bereit.

Prüfstandards

Funktionale Sicherheit

Die Prüfung der Funktionalen Sicherheit wurde auf Basis des international als Stand der Technik anerkannten Standards IEC 61508 durchgeführt. Um den Anforderungen des US amerikanischen Marktes gerecht zu werden, wurde zudem die UL 1998 herangezogen.

Primäre Sicherheit

Zur Vervollständigung und Spezifikation der technischen Anforderungen aus den oben angeführten Normen und Richtlinien sind die einschlägigen Normen bezüglich der Primären Sicherheit zu erfüllen. Insbesondere ist die Fachgrundnorm EN 61131-2 und die UL 508 zu nennen.

Elektromagnetische Verträglichkeit

Zusätzlich zur Erfüllung der Anforderungen aus der EMV Richtlinie wurden die speziellen Anforderungen aus der EN 61131-2 berücksichtigt.

Anwendungsbezogene Normen

Aufgrund der unterschiedlichen Anwendungsmöglichkeiten des Systems werden sowohl europäische (z.B. EN 60204-1 und EN 954-1) als auch amerikanische (z.B. NFPA 79) Normen hinsichtlich Maschinensicherheit betrachtet.

Für die Feuerungstechnik kommt im wesentlichen die EN 298 in Betracht.

Zusammenfassung

Die SIMATIC S7 Distributed Safety stellt aufgrund des Ansatzes der verteilten Struktur und den Einsatz diversitärer SW Strukturen einen Meilenstein in Hinblick auf zertifizierte Systeme dar. Auch die Möglichkeit sichere und nicht sichere Komponenten zu kombinieren bringt erhebliche Vorteile. Wegen der breit angelegten Prüfgrundlagen ist der Einsatz des Systems in vielen verschieden Anwendungen möglich. Das wird auch durch Anerkennung nach UL Standards unterstützt.

Weitere Informationen zu Services des TÜV SÜD in Hinblick auf Systeme und Applikationen:

www.tuev-sued.de/iqse

1.1 Allgemeines

1.2 Vorschriften und Normen in der Europäischen Union (EU)

1.3 Gesetzliche Anforderungen und Standard zur Sicherheit am Arbeitsplatz in Nordamerika

1.4 Sicherheitsanforderungen für Maschinen in Japan

1.5 Wichtige Adressen

1 Vorschriften und Normen

1 Vorschriften und Normen

1.1 Allgemeines

Zielsetzung

Zielsetzung der Sicherheitstechnik soll es sein, die Gefährdung von Menschen und Umwelt durch technische Einrichtungen so gering wie möglich zu halten, ohne dadurch die industrielle Produktion, den Einsatz von Maschinen oder die Herstellung von chemischen Produkten mehr als unbedingt notwendig einzuschränken. Durch international abgestimmte Regelwerke soll der Schutz von Mensch und Umwelt allen Ländern in gleichem Maße zuteil werden und gleichzeitig sollen Wettbewerbsverzerrungen wegen unterschiedlicher Sicherheitsanforderungen im internationalen Handel vermieden werden.

In den verschiedenen Regionen und Ländern der Welt gibt es unterschiedliche Konzepte und Anforderungen zur Gewährleistung von Sicherheit. Die rechtlichen Konzepte und die Anforderungen wie und wann nachzuweisen ist, ob ausreichende Sicherheit besteht, sind ebenso unterschiedlich wie die Zuordnung der Verantwortlichkeiten. So bestehen z.B. in der EU Anforderungen sowohl an den Hersteller einer Einrichtung als auch an den Betreiber, die durch europäische Richtlinien, Gesetze und Normen geregelt sind. In USA bestehen dagegen regional und sogar lokal unterschiedliche Anforderungen.

* EUC: Equipment under control

** E/E/PE: Electrical, electronic, programmable electronic

1) entspricht ISO 13849

2) auch EN 61508 und DIN EN 61508 / VDE 0803]]

Einheitlich im ganzen Land ist jedoch der Grundsatz, dass ein Arbeitgeber Sicherheit am Arbeitsplatz gewährleisten muss. Im Falle eines Schadens kann, aufgrund der Produkthaftung, der Hersteller für den Schaden, der mit seinem Produkt in Verbindung gebracht werden kann, haftbar gemacht werden. In anderen Ländern oder Regionen gelten wiederum andere Prinzipien.

Wichtig für Hersteller von Maschinen und Errichter von Anlagen ist, dass immer die Gesetze und Regeln des Ortes gelten, an dem die Maschine oder Anlage betrieben wird. Beispielsweise muss die Steuerung einer Maschine, die in USA betrieben werden soll, den dortigen Anforderungen genügen, auch wenn der Maschinenhersteller aus der EU stammt. Auch wenn die technischen Konzepte, mit denen Sicherheit erreicht wird, technischen Gesetzmäßigkeiten unterliegen, ist es trotzdem wichtig zu beachten, ob gesetzliche Regelungen mit bestimmten Vorgaben oder Restriktionen bestehen.

Funktionale Sicherheit

Die Sicherheit ist aus Sicht des zu schützenden Gutes unteilbar. Da die Ursachen von Gefährdungen und damit auch die technischen Maßnahmen zu ihrer Vermeidung aber sehr unterschiedlich sein können, unterscheidet man verschiedene Arten der Sicherheit, z.B. durch Angabe der jeweiligen Ursache möglicher Gefährdungen. So spricht man von „elektrischer Sicherheit“, wenn der Schutz vor den Gefährdungen durch die Elektrizität zum Ausdruck gebracht werden soll, oder von „funktionaler Sicherheit“, wenn die Sicherheit von der korrekten Funktion abhängt.

Diese Unterscheidung hat sich in der neueren Normung in der Art niedergeschlagen, dass es spezielle Normen gibt, die sich mit der funktionalen Sicherheit befassen. Im Bereich der Maschinensicherheit behandeln EN 954 [1)] und IEC 62061speziell die Anforderungen an sicherheitsrelevante Steuerungen und konzentriert sich damit auf die funktionale Sicherheit. IEC behandelt in der Basis Sicherheitsnorm IEC 61508 [2)] funktionale Sicherheit elektrischer, elektronischer und programmierbarer elektronischer Systeme unabhängig von einem speziellen Anwendungsgebiet.

Funktionale Sicherheit ist in IEC 61508 definiert als „part of the overall safety relating to the EUC* and the EUC control system which depends on the correct functioning of the E/E/PE** safety-related systems, other technology safety-related systems and external risk reduction facilities”.

Umfunktionale Sicherheit einer Maschine oder Anlage zu erreichen, ist es notwendig, dass die sicherheitsrelevanten Teile der Schutz- und Steuereinrichtungen korrekt funktionieren und sich im Fehlerfall so verhalten, dass die Anlage in einem sicheren Zustand bleibt oder in einen sicheren Zustand gebracht wird.

Dazu ist die Verwendung besonders qualifizierter Technik notwendig, die den in den betreffenden Normen beschriebenen Anforderungen genügt. Die Anforderungen zur Erzielung funktionaler Sicherheit basieren auf den grundlegenden Zielen:

- Vermeidung systematischer Fehler,
- Beherrschung systematischer Fehler,
- Beherrschung zufälliger Fehler oder Ausfälle.

Das Maß für die erreichte funktionale Sicherheit ist die Wahrscheinlichkeit gefährlicher Ausfälle, die Fehlertoleranz und die Qualität, durch die die Freiheit von systematischen Fehlern gewährleistet werden soll. Es wird in den Normen durch unterschiedliche Begriffe ausgedrückt. In IEC 61508: „Safety Integrity Level" (SIL), in EN 954: „Kategorien" und ISO 13849-1" Performance Level" (PL) (noch nicht verabschiedet).

Zielsetzung der Normen

Aus der Verantwortung, die Hersteller und Betreiber technischer Einrichtungen und Produkte für die Sicherheit haben, resultiert die Forderung, Anlagen, Maschinen und andere technische Einrichtungen so sicher zu machen, wie es nach dem Stand der Technik möglich ist. Dazu wird von den Wirtschaftspartnern der Stand der Technik bezüglich aller Aspekte, die für die Sicherheit von Bedeutung sind, in Normen beschrieben. Durch Einhaltung der jeweils relevanten Normen kann dann sichergestellt werden, dass der Stand der Technik erreicht ist und damit der Errichter einer Anlage oder Hersteller einer Maschine oder eines Gerätes seine Sorgfaltspflicht erfüllt hat.

Hinweis: Die in diesem Handbuch aufgeführten Normen, Richtlinien und Gesetze sind eine Auswahl, um wesentliche Ziele und Prinzipien zu vermitteln. Die Liste erhebt keinen Anspruch auf Vollständigkeit.

1.2 Vorschriften und Normen in der Europäischen Union (EU)

Grundprinzipien der gesetzlichen Anforderungen in Europa*

Die Gesetzgeber fordern, „durch vorbeugende Maßnahmen die Qualität der Umwelt und die Gesundheit des Menschen zu schützen" (Richtlinie 96/82/EG des Rates „Seveso II").

Sie fordern weiter „Sicherheit und Gesundheitsschutz der Beschäftigten bei der Arbeit" (Maschinenrichtlinie, Arbeitsschutzgesetze, ...). Die Erreichung dieser und ähnlicher Ziele wird in (EU-)Richtlinien vom Gesetzgeber für verschiedene Gebiete gefordert („geregelter Bereich"). Zur Erreichung dieser Ziele stellt der Gesetzgeber Anforderungen an die Betreiber von Anlagen und die Hersteller von Geräten und Maschinen und hat gleichzeitig die Verantwortung für mögliche Schäden zugeordnet.

Die EU-Richtlinien

- legen Anforderungen an Anlagen und deren Betreiber zum Schutz der Gesundheit der Menschen und der Qualität der Umwelt fest;

- enthalten Bestimmungen über die Sicherheit am Arbeitsplatz (Mindestanforderungen);

- legen Produktanforderungen (z.B. für Maschinen) zum Schutz der Sicherheit und Gesundheit der Verbraucher fest;

* Die EFTA-Staaten haben sich dem Konzept der EU angeschlossen.

- unterscheiden Anforderungen an die Realisierung von Produkten zur Gewährleistung des freien Warenverkehrs und Anforderungen an die Benutzung von Produkten.

Die EU-Richtlinen, die die Realisierung von Produkten betreffen, basieren auf Artikel 95 des EU-Vertrages, der den freien Warenverkehr regelt. Ihnen liegt ein neues, globales Konzept („new approach", „global approach") zugrunde:

- EU-Richtlinien enthalten nur allgemeine Sicherheitsziele und legen grundlegende Sicherheitsanforderungen fest.

- Technische Details können von Normungsgremien, die ein entsprechendes Mandat der EU-Kommission haben (CEN, CENELEC), in Normen festgelegt werden. Diese Normen werden unter einer bestimmten Richtlinie harmonisiert und im Amtsblatt der EU gelistet. Bei Erfüllung der harmonisierten Normen gilt die Vermutung, dass die betreffenden Sicherheitsanforderungen der Richtlinien erfüllt sind. (Näheres siehe "Maschinensicherheit in Europa")

- Die Einhaltung bestimmter Normen ist nicht vom Gesetzgeber vorgeschrieben. Aber bei Einhaltung bestimmter Normen „darf vermutet werden", dass die betreffenden Sicherheitsziele der EU-Richtlinien erfüllt sind.

- EU-Richtlinien verlangen von den Mitgliedsländern die gegenseitige Anerkennung nationaler Vorschriften.

Neben den gerätetypspezifischen Richtlinien wie z.B. Niederspannungsrichtlinie oder Maschinenrichtlinie, auf die im Folgenden näher eingegangen wird, gibt es auch eine allgemeine „Produktsicherheitsrichtlinie" (2001/95/EG), in der allgemeine Fragen zur Produktsicherheit geregelt sind. Sie ist in Deutschland im neuen (05.2004) Geräte- und Produktsicherheitsgesetz (GPSG) umgesetzt.

Die EU-Richtlinien sind nebeneinander gleichwertig, d.h., wenn mehrere Richtlinien für eine bestimmte Einrichtung zutreffen, gelten die Anforderungen aller relevanten Richtlinien (z.B. für eine Maschine mit elektrischer Ausrüstung gilt die Maschinenrichtlinie und die Niederspannungsrichtlinie).

Für Einrichtungen, die nicht zum Geltungsbereich der EU-Richtlinien gehören, gibt es Verordnungen. Sie enthalten Bestimmungen und Kriterien für freiwillige Prüfungen und Zertifizierungen.

Die EU-Richtlinien des New Approach mit den zugehörigen Listen der harmonisierten Normen findet man im Internet unter:

http://www.newapproach.org/

Niederspannungsrichtlinie

Die Niederspannungsrichtlinie (73/23/EEC) gilt für elektrische Einrichtungen mit Nennspannungen im Bereich 50 - 1000 V Wechselstrom bzw. 75 - 1500 V Gleichstrom (bei der z.Zt. erarbeiteten Neufassung werden die unteren Spannungsgrenzen entfallen).

Sie ist eine Richtlinie des New Approach. Für „elektrische Ausrüstung von Maschinen" ist EN 60204-1 unter der Niederspannungsrichtlinie gelistet. D.h. bei Erfüllung von EN 60204-1 darf vermutet werden, dass die Richtlinie erfüllt ist.

(Hinweis: Die Anforderungen zur Erfüllung der Niederspannungsrichtlinie werden in diesem Handbuch nicht näher behandelt.)

Arbeitsschutz in der EU

Die Anforderungen zur Sicherheit am Arbeitsplatz basieren auf Artikel 137 (früher 118a) des EU-Vertrages. Die Rahmenrichtlinie „Sicherheits- und Gesundheitsschutz der Arbeitnehmer" (89/391/EWG) legt Mindestanforderungen für Sicherheit am Arbeitsplatz fest. Die tatsächlichen Anforderungen unterliegen der nationalen Gesetzgebung und können die Anforderungen der Rahmenrichtlinie übersteigen. Diese Anforderungen betreffen das Betreiben von Produkten (z.B. Maschinen, Chemieanlagen), nicht deren Realisierung.

In Deutschland sind die Anforderungen in der Betriebssicherheitsverordnung (BetrSichV) zusammengefasst. Nähere Informationen dazu finden sich auf den Internetseiten der Bundesanstalt für Arbeitsschutz und Arbeitsmedizin (BauA)

(http://www.baua.de/baua/index.htm)

Maschinensicherheit in Europa

Maschinenrichtlinie (98/37/EG)*

Mit der Einführung des einheitlichen europäischen Binnenmarktes wurde beschlossen, dass die nationalen Normen und Vorschriften aller EG-Mitgliedsstaaten, die die technische Realisierung von Maschinen betreffen, harmonisiert werden. Dies hatte zur Folge, dass die Maschinenrichtlinie als eine Binnenmarktrichtlinie von den einzelnen Mitgliedsstaaten inhaltlich in nationales Recht umgesetzt werden musste. In Deutschland wurde der Inhalt der Maschinenrichtlinie als 9. Verordnung zum Gerätesicherheitsgesetz umgesetzt. Dies geschah bei der Maschinenrichtlinie vor dem Hintergrund einheitlicher Schutzziele mit dem Zweck, technische Handelshemmnisse abzubauen. Der Anwendungsbereich der Maschinenrichtlinie ist entsprechend ihrer Definition „Maschine ist eine Gesamtheit von miteinander verbundenen Teilen oder Vorrichtungen, von denen mindestens eines beweglich ist“ sehr weit gefasst. Mit Änderungsrichtlinien wurde der Anwendungsbereich nachträglich auf „Sicherheitsbauteile“ und „auswechselbare Ausrüstungen“ ausgedehnt. Die Maschinenrichtlinie betrifft die Realisierung von Maschinen.

Als „Maschine“ wird auch eine Gesamtheit von Maschinen bezeichnet, die, damit sie zusammenwirken, so angeordnet sind und betätigt werden, dass sie als Gesamtheit funktionieren.

* In den zuständigen Gremien der EU wird z.Z. über eine Neufassung der Maschinenrichtlinie verhandelt. Verbindliche Aussagen über die zu erwartenden Änderungen und den Zeitpunkt ihres Erscheinens sind derzeit nicht möglich.

Maschinenrichtlinie

Anwendungsbereich, Inverkehrbringen, freier Warenverkehr, Schutzklausel Art. 1 – Art. 7	**Bescheinigungsverfahren Art. 8 – Art. 9**	**CE-Kennzeichnung, Schutz vor Willkür Art. 10 – Art. 12**	**Inkrafttreten, Übergangsbestimmungen, Aufhebung von Vorschriften Art. 13 – Art. 14**

Anhang		**Artikel**
I	Grundlegende Sicherheits- und Gesundheitsanforderungen für – Maschinen sowie • auswechselbare Ausrüstungen • Sicherheitsbauteile	3 5 10
II	Inhalt von 1. EG-Konformitätserklärungen für – Maschinen sowie • auswechselbare Ausrüstungen • Sicherheitsbauteile 2. Erklärungen des Herstellers für – bestimmte Maschinenteile – nicht funktionsfähige Maschinen	4 5 8 4
III	CE-Konformitätskennzeichnung	10
IV	Typen von Maschinen und Sicherheitstechniken, für die das Verfahren gemäß Artikel 8 zur Anwendung kommt.	
V	Unterlagen zur EG-Konformitätserklärung für – Maschinen sowie • auswechselbare Ausrüstungen • Sicherheitsbauteile	8
VI	EG-Baumusterprüfungen für – Maschinen sowie • auswechselbare Ausrüstungen • Sicherheitsbauteile	8
VII	Mindestkriterien für Prüfstellen	9

Bild 1/1
Übersicht der Maschinenrichtlinie

Der Anwendungsbereich der Maschinenrichtlinie erstreckt sich somit von einer einfachen Maschine bis hin zu einer Anlage.

Die Maschinenrichtlinie ist in 14 Artikeln aufgebaut und besitzt 7 Anhänge.

Die Erfüllung der grundlegenden Sicherheits- und Gesundheitsanforderungen in Anhang I der Richtlinie ist für die Sicherheit von Maschinen zwingend notwendig. Der Hersteller muss folgende Grundsätze für die Integration der Sicherheit beachten (Anhang I Absatz 1.1.2):

a) „Durch die Bauart der Maschine muss gewährleistet sein, dass **Betrieb**, **Rüsten** und **Wartung** bei bestimmungsgemäßer Verwendung ohne Gefährdung von Personen erfolgen.“
„Die Maßnahmen müssen...Unfallrisiken...ausschließen...“

b) „Bei der Wahl der angemessenen Lösungen muss der Hersteller folgende Grundsätze anwenden, und zwar in der angegebenen Reihenfolge:

- Beseitigung oder Minimierung der Gefahren (Integration des Sicherheitskonzepts in die Entwicklung und den Bau der Maschine);
- Ergreifen von notwendigen Schutzmaßnahmen gegen nicht zu beseitigende Gefahren;
- Unterrichtung der Benutzer über die Restgefahren aufgrund der nicht vollständigen Wirksamkeit der getroffenen Sicherheitsmaßnahmen.

Die Schutzziele müssen verantwortungsbewusst umgesetzt werden, um die Forderung nach Konformität mit der Richtlinie zu erfüllen.

Der Hersteller einer Maschine muss den Nachweis über die Übereinstimmung mit den grundlegenden Anforderungen erbringen. Dieser Nachweis wird durch die Anwendung harmonisierter Normen erleichtert.

Bei Maschinen nach Anhang IV der Maschinenrichtlinie, die ein größeres Gefahrenpotenzial darstellen, wird ein Bescheinigungsverfahren verlangt. (Empfehlung: Auch Maschinen, die nicht in Anhang IV aufgeführt sind, können ein großes Gefahrenpotenzial darstellen und sollten entsprechend behandelt werden.) Das genaue „Verfahren zur Feststellung der Übereinstimmung“ mit den Zielen ist im Kapitel II der Richtlinie festgelegt.

Bild 1/2
Anhang IV der Maschinenrichtlinie

Typen von Maschinen und Sicherheitsbauteilen, für die das Verfahren gemäß Artikel 8 Absatz 2 Buchstabe b) und c) zur Anwendung kommt.

A. Maschinen

1. (Einblatt- und Mehrblatt-)Kreissägen zum Bearbeiten von Holz und gleichartigen Werkstoffen oder zum Bearbeiten von Fleisch und gleichartigen Werkstoffen
1.1. Sägemaschinen mit während des Arbeitsvorgangs fest stehendem Werkzeug, mit fest stehendem Tisch, mit Handvorschub des Sägeguts oder mit abnehmbarem Vorschubapparat
1.2. Sägemaschinen mit während des Arbeitsvorgangs fest stehendem Werkzeug, mit Pendelblock oder -schlitten, mit Handvorschub
1.3. Sägemaschinen mit während des Arbeitsvorgangs feststehendem Werkzeug, mit bauarteigenem mechanischem Vorschub des Sägeguts und Handbeschickung und/oder Handentnahme
1.4. Sägemaschinen mit während des Arbeitsvorgangs beweglichem Werkzeug, mit mechanischer Vorschubvorrichtung und Handbeschickung und/oder Handentnahme
2. Abrichthobel mit Handvorschub für die Holzbearbeitung
3. Hobelmaschinen für einseitige Bearbeitung mit Handbeschickung und/oder Handentnahme für die Holzbearbeitung
4. Bandsägen mit beweglichem oder unbeweglichem Sägetisch und Bandsägen mit beweglichem Schlitten mit Handbeschickung und/oder Handentnahme für das Bearbeiten von Holz und gleichartigen Werkstoffen oder für das Bearbeiten von Fleisch und gleichartigen Werkstoffen
5. Kombinierte Maschinen der unter den Nummern 1 bis 4 und Nummer 7 genannten Typen für die Bearbeitung von Holz und gleichartigen Werkstoffen
6. Mehrspindel-Zapfenfräsmaschinen mit Handvorschub für die Holzbearbeitung
7. Unterfräsmaschinen mit Handvorschub für die Bearbeitung von Holz und gleichartigen Werkstoffen
8. Handkettensägen für die Holzbearbeitung
9. Pressen einschließlich Biegepressen für die Kaltbearbeitung von Metall mit Handbeschickung und/oder Handentnahme, deren im Fertigungsvorgang bewegliche Teile einen Hub von mehr als 6 mm und eine Geschwindigkeit von mehr als 30 mm/s haben können
10. Kunststoffspritzgieß- oder -formpressmaschinen mit Handbeschickung oder Handentnahme
11. Gummispritzgieß- oder -formpressmaschinen mit Handbeschickung oder Handentnahme
12. Maschinen für den Einsatz unter Tage:
    – schienengeführte Maschinen: Lokomotiven und Bremswagen
    – hydraulischer Schreitausbau
    – Verbrennungsmotoren für die Ausrüstung von unter Tage einsetzbaren Maschinen
13. Hausmüllsammelwagen für manuelle Beschickung mit Pressvorrichtung
14. Abnehmbare Schutzeinrichtungen und Kardanwellen zur Kraftübertragung gemäß Nummer 3.4.7.
15. Hebebühnen für Fahrzeuge
16. Maschinen zum Heben von Personen, bei denen die Gefahr eines Absturzes aus einer Höhe von mehr als 3 m besteht
17. Maschinen für die Herstellung von pyrotechnischen Sätzen

B. Sicherheitsbauteile

1. Elektrosensible Personenschutzeinrichtungen, z. B. Lichtschranken, Schaltmatten, elektromagnetische Detektoren
2. Logikeinheiten zur Aufrechterhaltung der Sicherheitsfunktionen von Zweihandschaltungen
3. Selbsttätige bewegliche Schutzeinrichtungen an Maschinen gemäß Buchstabe A Nummer 9, 10 und 11
4. Überrollschutzaufbau (ROPS)
5. Schutzaufbau gegen herabfallende Gegenstände (FOPS)

Die Maschinenrichtlinie definiert in Kapitel 1 Artikle 1 (2):

B. „Sicherheitsbauteil"

soweit es sich nicht um eine auswechselbare Ausrüstung handelt, ein Bauteil, das vom Hersteller ... mit dem Verwendungszweck der Gewährleistung einer Sicherheitsfunktion in den Verkehr gebracht wird und dessen Ausfall oder Fehlfunktion die Sicherheit oder die Gesundheit der Personen im Wirkbereich der Maschine gefährdet.

Zusammen mit den Erläuterungen zur MR kann das folgendermaßen interpretiert werden.

„Sicherheitsbauteile sind dadurch charakterisiert, dass sie eine vom Hersteller angegebene entsprechende (als Sicherheitsbauteil) Zweckbestimmung im Sinne der Richtlinie haben müssen. In den Erläuterungen zur Richtlinie wird in Abschnitt 76 festgestellt, dass Bauteile, „die eine Betriebsfunktion zu erfüllen haben" keine Sicherheitsbauteile sind. Dies gilt auch dann, wenn deren Versagen zu einer Gefährdung führen würde und diese selbstverständlich sicher sein müssen. Als Beispiel für ein Nicht- Sicherheitsbauteil in diesem Sinne wird in Abschnitt 81 der Erläuterungen das Hubseil [eines Krans] genannt. Hauptfunktion des Seils ist das betriebsmäßige Heben und Senken von Lasten, nicht aber die ebenfalls gegebene „Sicherung gegen Lastabsturz". Übertragen z.B. auf Antriebe bedeutet dies, dass diese in der Regel keine Sicherheitsbauteile sind, da Ihre Hauptfunktion eindeutig im normalen Maschinenbetrieb liegt.

Andererseits werden Bauteile mit Doppelfunktion, wie zum Beispiel Zweihandschaltungen, dann als Sicherheitsbauteil betrachtet, wenn die Sicherheitsfunktion (Schutz des Bedieners) gegenüber der Betriebsfunktion (Auslösen eines Arbeitsvorganges) von überragender Bedeutung ist (Abschnitt 80 der Erläuterungen zur Maschinenrichtlinie).

Einzelteile, die des Zusammenbaus mit weiteren, getrennt zu beschaffenden Teilen oder Softwareprogrammen bedürfen, um eine Sicherheitsfunktion zu realisieren, können selbst keine Sicherheitsbauteile sein. Dies gilt auch dann, wenn diese Einzelteile ausdrücklich zur Verwendung in Sicherheitsbauteilen vorgesehen sind.

Normen

Um Produkte in den Verkehr bringen oder betreiben zu dürfen, müssen sie den grundlegenden Sicherheitsanforderungen der EU-Richtlinien entsprechen. Zur Erfüllung dieser Sicherheitsanforderungen können Normen sehr hilfreich sein. Dabei ist in der EU zu unterscheiden zwischen Normen, die unter einer EU-Richtlinie harmonisiert sind und Normen, die zwar ratifiziert, aber nicht unter einer bestimmten Richtlinie harmonisiert sind, sowie sonstigen technischen Regeln, in den Richtlinien auch „nationale Normen" genannt.

Ratifizierte Normen beschreiben den anerkannten Stand der Technik. D.h. der Hersteller kann durch ihre Anwendung nachweisen, dass er den anerkannten Stand der Technik erfüllt hat.

Grundsätzlich müssen alle Normen, die als Europanormen ratifiziert sind, in die nationalen Normenwerke der Mitgliedsstaaten unverändert übernommen werden, unabhängig davon, ob sie unter einer Richtlinie harmonisiert sind oder nicht. Bestehende nationale Normen zum gleichen Thema müssen dann zurückgezogen werden. So soll im Laufe der Zeit in Europa ein einheitliches (widerspruchsfreies) Normenwerk geschaffen werden.

Hinweis: Eine wichtige nicht unter einer EU-Richtlinie harmonisierte Norm ist IEC 61508 „Functional safety of electrical/electronic/programmable electronic safety-related systems". Sie ist als EN 61508 ratifiziert. (Die deutschen Vornormen DIN V VDE 0801 und DIN V 19250 und 19251 wurden deshalb bis August 2004 zurückgezogen.) Dort, wo EN 61508 in einer harmonisierten Norm referenziert wird, ist sie eine „mitgeltende" Norm zu der betreffenden harmonisierten Norm.

Harmonisierte Europanormen

Sie werden von den beiden Normungsorganisationen CEN (Comité Européen de Normalisation) und CENELEC (Comité Européen de Normalisation Électrotechnique) im Auftrag der EU-Kommission erarbeitet, um die Anforderungen der EU-Richtlinien für ein bestimmtes Produkt zu präzisieren. Diese Normen (EN-Normen) werden im Amtsblatt der europäischen Gemeinschaften veröffentlicht und sind danach ohne Änderungen in nationale Normen zu übernehmen

Sie dienen zur Erfüllung der grundlegenden Sicherheits- und Gesundheitsanforderungen und der im Anhang I der Maschinenrichtlinie genannten Schutzziele.

Der Ansprechpartner für CEN/CENELEC in Deutschland ist das DIN und die DKE.

Durch Einhaltung der harmonisierten Normen ergibt sich eine „automatische Vermutungswirkung" der Erfüllung der Richtlinie, d.h., der Hersteller darf darauf vertrauen, dass er die Sicherheitsaspekte der Richtlinie erfüllt hat, soweit sie in der jeweiligen Norm behandelt sind. Allerdings ist nicht jede Europanorm in diesem Sinne harmonisiert. Entscheidend ist die Listung im europäischen Amtsblatt. Diese Listen sind stets aktuell im Internet abrufbar

(Adresse:
http://www.newapproach.org/)

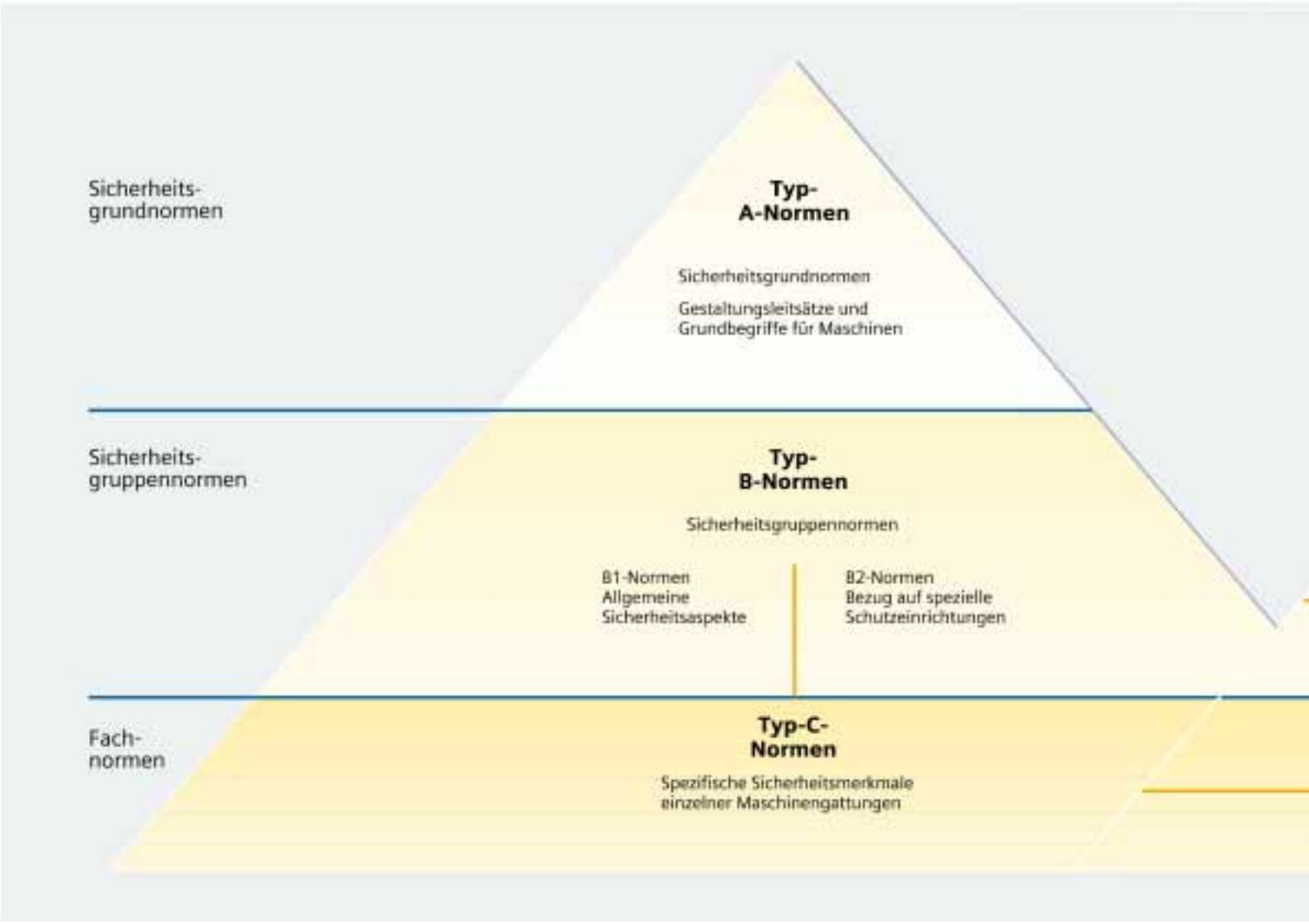


Bild 1/3
Das europäische Normenwerk für Sicherheit von Maschinen

Das europäische Normenwerk für Sicherheit von Maschinen ist hierarchisch aufgebaut, es gliedert sich in

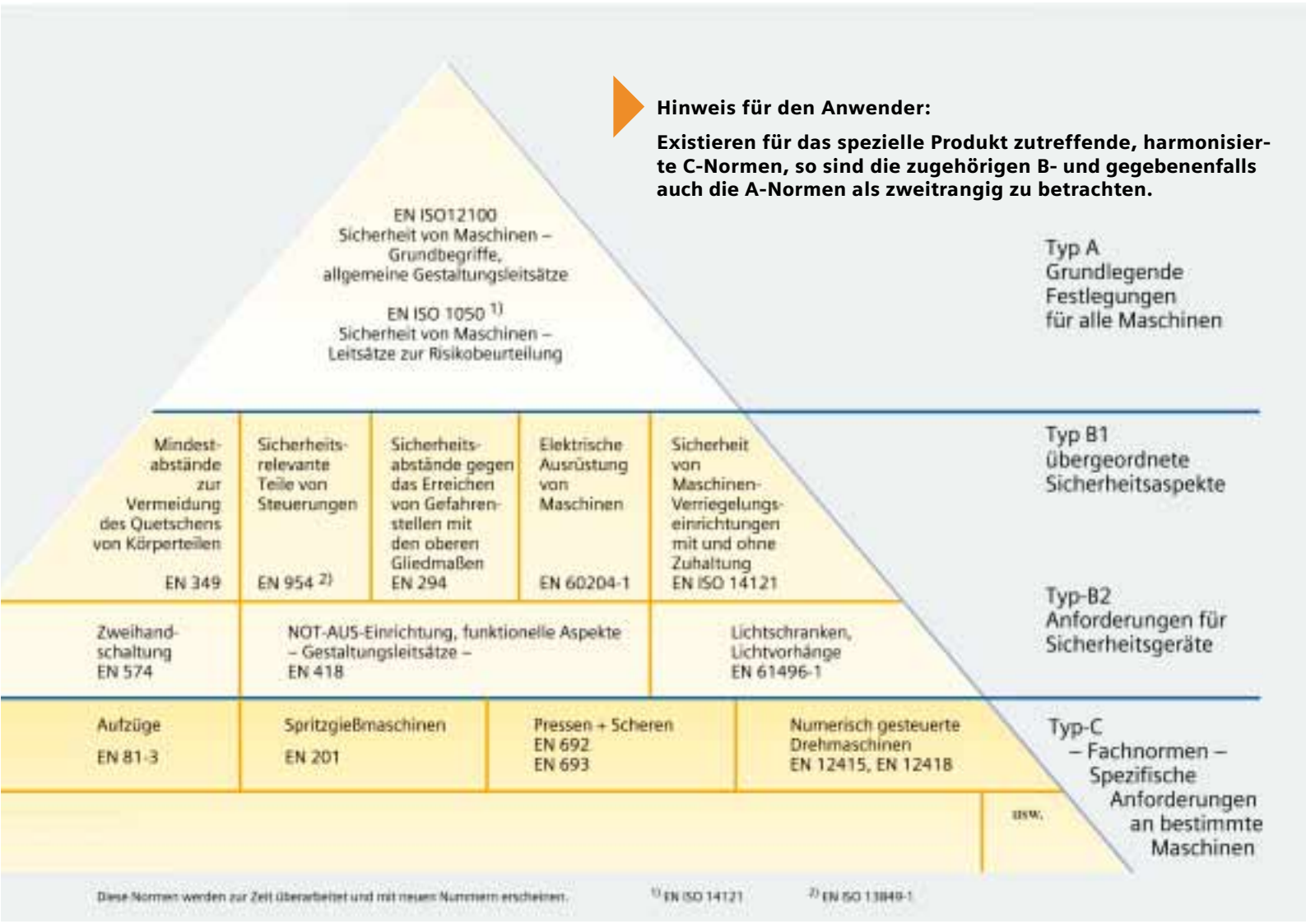
- A-Normen,
  auch Grundnormen genannt.
- B-Normen,
  auch Gruppennormen genannt.
- C-Normen,
  auch Produktnormen genannt.

Den Aufbau zeigt die obige Darstellung.

Zu Typ-A-Normen/Grundnormen

A-Normen enthalten grundlegende Begriffe und Festlegungen für alle Maschinen. Dazu zählt die EN ISO 12100 (früher EN 292) „Sicherheit von Maschinen, Grundbegriffe, allgemeine Gestaltungsleitsätze."

A-Normen richten sich primär an die Normensetzer von B- und C-Normen. Die dort niedergelegten Verfahren zur Risikominimierung können jedoch auch für den Hersteller hilfreich sein, wenn keine C-Normen vorliegen.



Zu Typ-B-Normen/Gruppennormen

Das sind alle Normen mit sicherheitstechnischen Aussagen, die mehrere Arten von Maschinen betreffen können.

Auch die B-Normen richten sich primär an die Normensetzer für C-Normen. Sie können jedoch auch für Hersteller bei Konstruktion und Bau einer Maschine hilfreich sein, wenn keine C-Normen vorliegen.

Es wurde bei den B-Normen eine weitere Unterteilung vorgenommen, und zwar in:

Typ-B1-Normen für übergeordnete Sicherheitsaspekte, z.B. ergonomische Grundsätze, Sicherheitsabstände gegen das Erreichen von Gefahrquellen, Mindestabstände zur Vermeidung des Quetschens von Körperteilen.

Typ-B2-Normen für Sicherheitseinrichtungen sind bestimmt für verschiedene Maschinenarten, z.B. Not-Halt- Einrichtungen, Zweihandschaltungen, Verriegelungen, berührungslos wirkende Schutzeinrichtungen, sicherheitsbezogene Teile von Steuerungen.

Zu Typ-C-Normen/Produktnormen

Hierbei handelt es sich um maschinenspezifische Normen z.B. für Werkzeugmaschinen, Holzbearbeitungsmaschinen, Aufzüge, Verpackungsmaschinen, Druckmaschinen u.ä.

Das europäische Normenwerk ist so aufgebaut, dass, um Wiederholungen allgemeiner Aussagen zu vermeiden, die in Typ-A- oder Typ-B-Normen bereits enthalten sind, in den Typ- C-Normen soweit wie möglich darauf verwiesen wird.

Produktnormen enthalten maschinenspezifische Anforderungen. Die Anforderungen können unter Umständen von den Grund- und Gruppennormen abweichen. Für den Maschinenbauer hat die Typ-C-Norm/Produktnorm die absolut höhere Priorität. Er darf davon ausgehen, dass er damit die grundlegenden Anforderungen des Anhangs I der Maschinenrichtlinien einhält (automatische Vermutungswirkung). Liegt für eine Maschine keine Produktnorm vor, so können Typ-B-Normen als Hilfen für den Bau einer Maschine herangezogen werden.

Um ein Mittel der Übereinstimmung mit den grundlegenden Anforderungen der Richtlinie bereitzustellen, werden für Maschinen oder Maschinengruppen nahezu aller Bereiche mit dem Mandat der EG-Komission harmonisierte Normen in technischen Komitees des CEN und CENELEC erarbeitet. An der Erarbeitung sind in erster Linie Vertreter der Hersteller der betreffenden Maschinen, der Aufsichtsbehörden wie Berufsgenossenschaften sowie der Betreiber beteiligt. Eine vollständige Liste aller gelisteten Normen sowie der mandatierten Normungsvorhaben finden Sie im Internet unter:

http://www.newapproach.org/

Empfehlung: Wegen der rasch fortschreitenden technischen Entwicklung und den damit verbundenen Änderungen von Maschinenkonzepten sollte bei Anwendung besonders von C-Normen deren Aktualität geprüft werden. Gegebenenfalls ist zu beachten, dass die Anwendung der Norm nicht zwingend ist, sondern das Sicherheitsziel erreicht werden muss.

Nationale Normen

Fehlen harmonisierte Europanormen oder können sie aus bestimmten Gründen nicht angewendet werden, so kann sich ein Hersteller der „nationalen Normen" bedienen. Unter diesen Begriff der Maschinenrichtlinie fallen alle anderen technischen Regeln, z.B. auch die Unfallverhütungsvorschriften und nicht im europäischen Amtsblatt gelistete Normen (auch IEC- oder ISO-Normen, die als EN ratifiziert wurden). Durch Anwendung ratifizierter Normen kann der Hersteller nachweisen, dass der anerkannte Stand der Technik erfüllt wurde. Die Anwendung dieser Normen ergibt allerdings nicht die oben erwähnte „automatische Vermutungswirkung".

Risikoanalyse/-beurteilung

Maschinen und Anlagen beinhalten, aufgrund ihres Aufbaus und ihrer Funktionalität, Risiken. Deshalb verlangt die Maschinenrichtlinie für jede Maschine eine Risikobeurteilung und gegebenenfalls eine Risikominderung, bis das Restrisiko kleiner als das tolerierbare Risiko ist. Für die Verfahren der Bewertung dieser Risiken sind die Normen

- EN ISO 12100 „Sicherheit von Maschinen – Grundbegriffe, allgemeine Gestaltungsleitsätze" und
- EN 1050 „Sicherheit von Maschinen, Leitsätze zur Risikobeurteilung"

anzuwenden.

Schwerpunktmäßig beschreibt EN ISO 12100 die zu betrachtenden Risiken und Gestaltungsleitsätze zur Risikominderung, EN 1050 den iterativen Prozess mit Risikobeurteilung und Risikominderung zum Erreichen der Sicherheit. (Zur Erläuterung dieses Verfahrens siehe Kapitel 2.)

Risikobeurteilung

Die Risikobeurteilung ist eine Folge von Schritten, welche die systematische Untersuchung von Gefährdungen erlauben, die von Maschinen ausgehen. Wo notwendig, folgt einer Risikobeurteilung eine Risikoreduzierung. Bei Wiederholung dieses Vorgangs ergibt sich der iterative Prozess (siehe Bild 1/5), mit dessen Hilfe Gefährdungen so weit wie möglich beseitigt werden können und entsprechende Schutzmaßnahmen getroffen werden können.

Die Risikobeurteilung umfasst die

- Risikoanalyse
  a) Bestimmung der Grenzen der Maschine (EN ISO 12100, EN 1050 Abs. 5)
  b) Identifizierung der Gefährdungen (EN ISO 12100, EN 1050 Abs. 6)
  c) Verfahren zur Risikoeinschätzung (EN 1050 Abs. 7)
- Risikobewertung (EN 1050 Abs. 8)

Gemäß dem iterativen Prozess zum Erreichen der Sicherheit erfolgt nach der Risikoeinschätzung eine Risikobewertung. Dabei muss entschieden

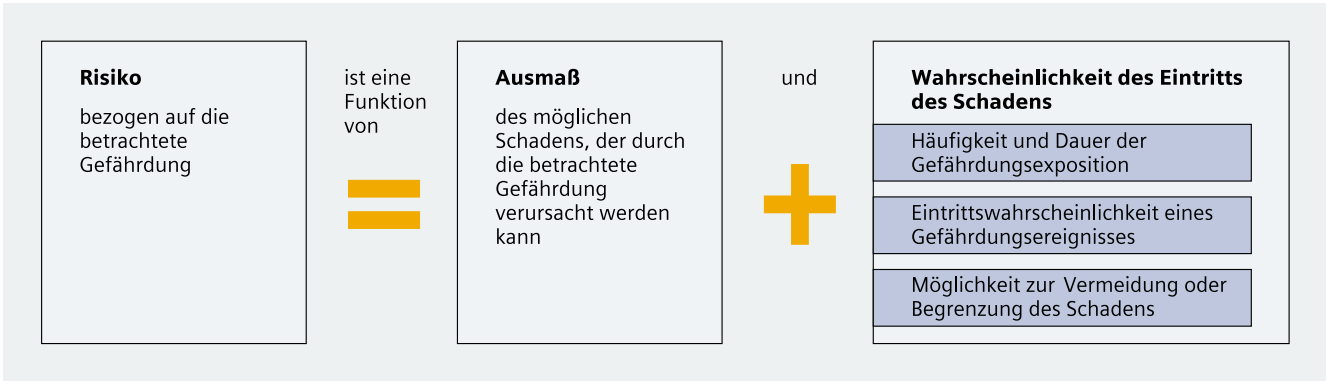

Risiko
bezogen auf die betrachtete Gefährdung
ist eine Funktion von
Ausmaß
des möglichen Schadens, der durch die betrachtete Gefährdung verursacht werden kann
und
Wahrscheinlichkeit des Eintritts des Schadens
Häufigkeit und Dauer der Gefährdungsexposition
Eintrittswahrscheinlichkeit eines Gefährdungsereignisses
Möglichkeit zur Vermeidung oder Begrenzung des Schadens

Bild 1/4
Risikoelemente

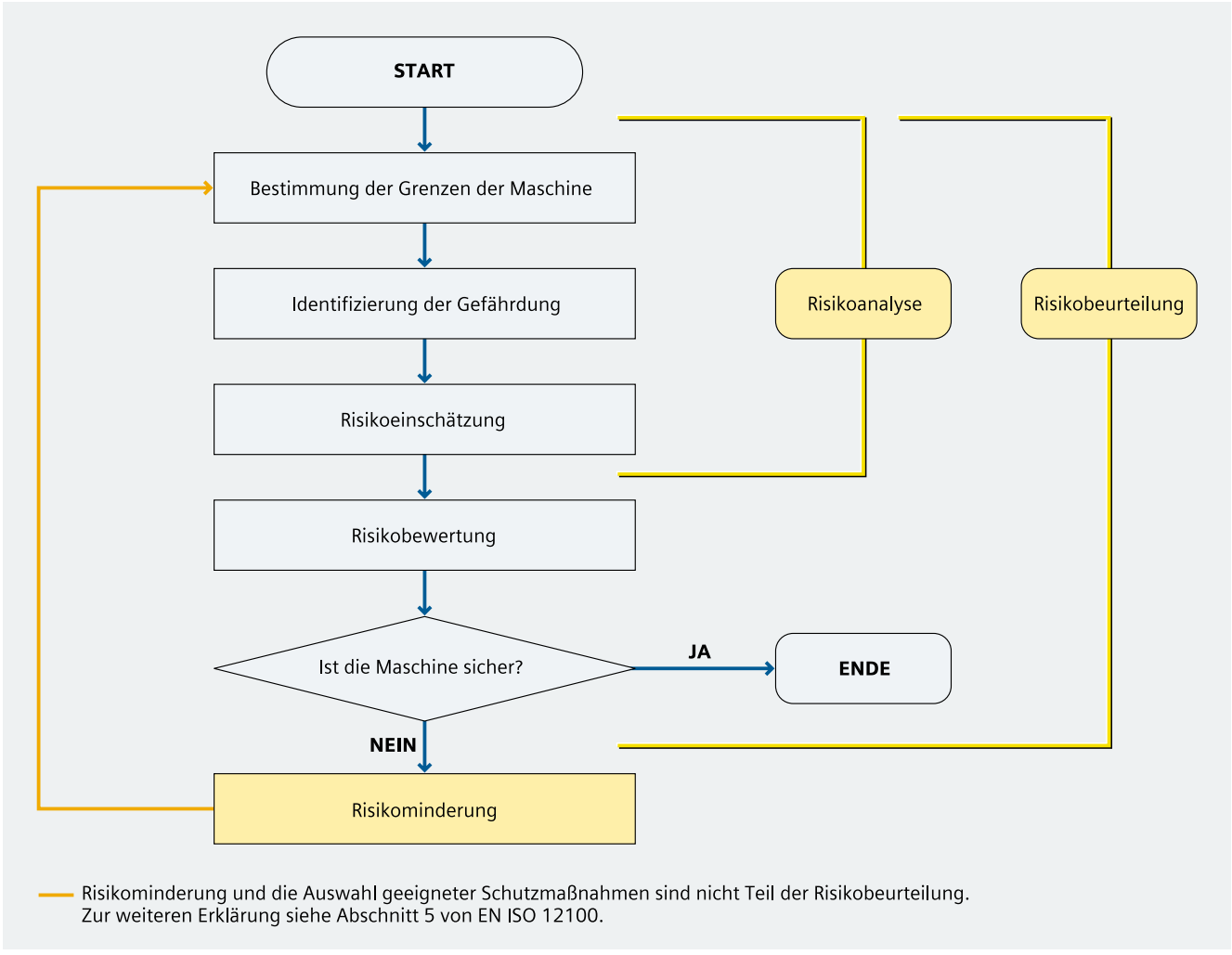


Bild 1/5
Iterativer Prozess zum Erreichen der Sicherheit nach EN 1050
Hinweis: Die in EN 1050 referenzierten EN 292-1 /-2 sind inzwischen durch EN ISO 12100-1 /-2 ersetzt.

werden, ob eine Risikominderung notwendig ist. Falls das Risiko weiter vermindert werden soll, sind geeignete Schutzmaßnahmen auszuwählen und anzuwenden. Die Risikobeurteilung ist dann zu wiederholen.

Als Hilfe zur Risikobewertung sind Risikoelemente definiert. Den Zusammenhang dieser Risikoelemente verdeutlicht Bild 1/4.

Ist die erforderliche Sicherheit noch nicht erreicht, sind Maßnahmen zur Risikominderung erforderlich.

Die Risikominderung muss durch geeignete Konzipierung und Realisierung der Maschine erfolgen, z.B. durch für Sicherheitsfunktionen geeignete Steuerung oder Schutzmaßnahmen (siehe dazu Abschnitt „Anforderungen der Maschinenrichtlinie"). Umfassen die Schutzmaßnahmen Verriegelungs- oder Steuerfunktionen, sind diese gemäß EN 954 zu gestalten. Dabei müssen elektronische Steuerungen und Bussysteme außerdem IEC / EN 61508 erfüllen. Für elektrische und elektronische Steuerungen kann EN 62061 alternativ zu EN 954 verwendet werden.

Restrisiko (EN 1050)

Sicherheit ist ein relativer Begriff unserer technisierten Welt. Sicherheit so zu realisieren, dass unter keinen Umständen etwas passieren kann, sozusagen die „Null-Risiko-Garantie", ist leider nicht durchführbar. Das verbleibende Restrisiko ist definiert als: Risiko, das nach Ausführung der Schutzmaßnahmen verbleibt.
Hierbei sind unter Schutzmaßnahmen alle Maßnahmen zur Risikominderung zu verstehen.

Risikominderung

Die Risikominderung einer Maschine kann, außer durch strukturelle Maßnahmen, auch durch sicherheitsrelevante Steuerungsfunktionen erfolgen. Für die Realisierung dieser Steuerungsfunktionen sind, abgestuft nach der Höhe des Risikos, besondere Anforderungen zu beachten, die in EN 954-1 und, für elektrische Steuerungen insbesondere mit programmierbarer Elektronik, in IEC 61508 beschrieben sind.

Die Anforderungen an sicherheitsrelevante Teile von Steuerungen sind nach der Höhe des Risikos bzw. der notwendigen Risikominderung abgestuft.
EN 954-1 definiert dazu „Kategorien" und beschreibt in ihrem Anhang B ein Verfahren zur Auswahl der geeigneten Kategorie für die Gestaltung der sicherheitsbezogenen Teile einer Steuerung. Mit der Neufassung (EN ISO 13849-1) wird es einen neuen Risikographen geben, der anstelle der Kategorien zu hierarchisch abgestuften Performance Leveln führt.

IEC 62061 verwendet „Safety Integrity Level" (SIL) zur Abstufung. Das ist ein quantifiziertes Maß für die sicherheitsbezogene Leistungsfähigkeit einer Steuerung. Die Ermittlung des notwendigen SIL erfolgt ebenfalls nach dem Prinzip der Risikobewertung gemäß EN 1050. Im Anhang A der Norm ist ein Verfahren zur Bestimmung des notwendigen Safety Integrity Level (SIL) beschrieben.

Wichtig ist in jedem Fall, unabhängig davon welche Norm angewendet wird, dass alle Teile der Steuerung der Maschine, die an der Ausführung der sicherheitsrelevanten Funktionen beteiligt sind, diesen Anforderungen genügen.

Weitere Einzelheiten siehe Kapitel 2.

Hinweis: Zur Steuerung einer Maschine gehören auch die Laststromkreise der Antriebe und Motoren.

Beim Entwurf und der Realisierung der Steuerung ist es notwendig zu überprüfen, ob die Anforderungen der ausgewählten Kategorie bzw. des SIL erfüllt sind. Da die Anforderungen zur Erzielung der notwendigen Safety Performance in EN 954 und IEC unterschiedlich strukturiert sind, sind auch die Anforderungen zur Überprüfung unterschiedlich strukturiert. Für ein Design gemäß EN 954 sind die Einzelheiten für die Validierung und was dabei zu beachten ist, im Teil 2 (neue Bezeichnung EN ISO 13849-2) beschrieben. Die Anforderungen zur Validierung eines Design gemäß IEC 62061 sind in der Norm selbst beschrieben.

Die nebenstehende Tabelle zeigt eine Kurzfassung der Anforderungen für Kategorien gemäß EN 954-1: 1996. In den Kategorien sind grundlegende Anforderungen zur Gestaltung von Steuerungen festgelegt, die sie robust gegen Ausfälle der Hardware machen. Mit der bevorstehenden Neuausgabe als EN ISO 13849-1 werden sich diese Anforderungen zum Teil ändern.

Für komplexe Einrichtungen, insbesondere Steuerungen mit programmierbarer Elektronik, Bussysteme oder drehzahlveränderbare Antriebe, sind weitergehende Aspekte zu beachten, damit

- zufällige Ausfälle der Hardware beherrscht,
- systematische Fehler in der Hardware und der Software vermieden und

Kategorie[1]	Kurzfassung der Anforderungen	Systemverhalten[2]	Prinzipien zum Erreichen der Sicherheit
B	Die sicherheitsbezogenen Teile von Steuerungen und/oder ihre Schutzeinrichtungen als auch ihre Bauteile müssen in Übereinstimmung mit den zutreffenden Normen so gestaltet, gebaut, ausgewählt, zusammengestellt und kombiniert werden, dass sie den zu erwartenden Einflüssen standhalten können.	Das Auftreten eines Fehlers kann zum Verlust der Sicherheitsfunktion führen.	überwiegend durch Auswahl von Bauteilen charakterisiert
1	Die Anforderungen von B müssen erfüllt sein. **Bewährte Bauteile** und **bewährte Sicherheitsprinzipien** müssen angewendet werden.	Das Auftreten eines Fehlers kann zum Verlust der Sicherheitsfunktion führen, aber die Wahrscheinlichkeit des Auftretens ist geringer als in Kategorie B.	
2	Die Anforderungen von B und die Verwendung bewährter Sicherheitsprinzipien müssen erfüllt sein. Die Sicherheitsfunktion muss in geeigneten Zeitabständen durch die Maschinensteuerung geprüft werden.	– Das Auftreten eines Fehlers kann zum Verlust der Sicherheitsfunktion zwischen den Prüfungsabständen führen. – Der Verlust der Sicherheitsfunktion wird durch die Prüfung erkannt.	überwiegend durch die Struktur charakterisiert
3	Die Anforderungen von B und die Verwendung **bewährter Sicherheitsprinzipien** müssen erfüllt sein. Sicherheitsbezogene Teile müssen so gestaltet sein, dass: – ein einzelner Fehler in jedem dieser Teile nicht zum Verlust der Sicherheitsfunktion führt, und – wann immer in angemessener Weise durchführbar, der einzelne Fehler erkannt wird.	– Wenn der einzelne Fehler auftritt, bleibt die Sicherheitsfunktion immer erhalten. – Einige, aber nicht alle Fehler werden erkannt. – Eine Anhäufung unerkannter Fehler kann zum Verlust der Sicherheitsfunktion führen.	
4	Die Anforderungen von B und die Verwendung **bewährter Sicherheitsprinzipien** müssen erfüllt sein. Sicherheitsbezogene Teile müssen so gestaltet sein, dass: – ein einzelner Fehler in jedem dieser Teile nicht zum Verlust der Sicherheitsfunktion führt, und – der einzelne Fehler bei oder vor der nächsten Anforderung an die Sicherheitsfunktion erkannt wird oder, wenn dies nicht möglich ist, eine Anhäufung von Fehlern dann nicht zum Verlust der Sicherheitsfunktion führt.	– Wenn Fehler auftreten, bleibt die Sicherheitsfunktion immer erhalten. – Die Fehler werden rechtzeitig erkannt, um einen Verlust der Sicherheitsfunktion zu verhindern.	

[1] Die Kategorien sind nicht dazu bestimmt, in irgendeiner gegebenen Reihenfolge oder hierarchischen Anordnung in Bezug auf die sicherheitstechnischen Anforderungen angewendet zu werden.

[2] Aus der Risikobeurteilung wird sich ergeben, ob der gesamte oder teilweise Verlust der Sicherheitsfunktion(en) aufgrund von Fehlern akzeptabel ist.

Bild 1/6
Beschreibungen der Anforderungen für die Kategorien nach EN 954-1

- systematische Fehler in der Hardware und der Software beherrscht werden,

so dass sie ausreichend funktionssicher für sicherheitskritische Aufgaben sind. Die dazu notwendigen Anforderungen beschreibt die internationale Norm IEC 61508 (identisch IEC 61508) und für berührungslos wirkende Schutzeinrichtungen wie Lichtgitter oder Laserscanner IEC / EN 61496. Der Umfang der geforderten Maßnahmen ist auch hier entsprechend der verlangten Risikominderung abgestuft.

Die neuere technische Entwicklung ermöglicht die Anwendung komplexer Systeme für sicherheitsrelevante Funktionen, sofern diese den Anforderungen von IEC 61508 genügen. Um dem Rechnung zu tragen, wurde für Maschinensteuerungen die neue Norm IEC 62061 entwickelt und wird außerdem die bestehende EN 954-1 überarbeitet. Letztere wird mit den neuen Bezeichnung ISO 13849-1 erscheinen. Beide Normen sollen es dem Anwender ermöglichen, unter Verwendung geeigneter Geräte sicherheitsrelevante Steuerungen mit elektrischen und elektronischen Komponenten aufzubauen, ohne selber IEC 61508 anwenden zu müssen.

IEC 62061 setzt voraus, dass die eingesetzten elektronischen Geräte ihrerseits bereits IEC 61508 erfüllen und beschreibt ein Konzept zur Realisierung auch umfangreicher Sicherheitsfunktionen. Dieses Konzept richtet sich speziell an den Integrator von Maschinensteuerungen und ermöglicht die Quantifizierung der erreich-

ten Safety Performance ohne komplizierte Rechnungen.

Das Konzept der zukünftigen ISO 13849-1 beschränkt sich auf bestimmte einfache Architekturen und hat im wesentlichen die hierfür notwendigen Anforderungen aus IEC 61508 integriert. Die Anforderungen für sicherheitsrelevante Teile von Steuerungen auf Basis elektromechanischer Bauteile wurden gegenüber EN 954-1 ergänzt, so dass auch hier eine quantifizierte hierarchische Abstufung der Safety Performance ermöglicht wird.

Zur Entscheidung, ob ISO 13849 oder IEC 62061 angewendet werden soll, siehe Kapitel 2.

Validierung

Validierung bedeutet eine bewertende Überprüfung der angestrebten Sicherheitsfunktionalität. Ihr Zweck ist, die Festlegungen und das Niveau der Konformität der sicherheitsbezogenen Teile der Steuerung innerhalb der Gesamtfestlegung für Sicherheitsanforderungen an der Maschine zu bestätigen. Die Validierung muss weiterhin aufzeigen, dass jedes sicherheitsbezogene Teil die Anforderungen der relevanten Norm erfüllt. Dabei sind die folgenden Aspekte beschrieben:

- Fehlerlisten
- Validierung der Sicherheitsfunktionen
- Validierung der geforderten und der erreichten Safety Performance (Kategorie, Safety Integrity Level oder Performance level)
- Validierung der Umgebungsanforderungen
- Validierung der Instandhaltungsanforderungen

In einem Validierungsplan müssen die Anforderungen für die Durchführung der Validierung für die festgelegten Sicherheitsfunktionen beschrieben werden.

Safety Integrated

Die Maßnahmen, um eine komplexe Steuerung für Sicherheitsaufgaben ausreichend funktionssicher zu machen, sind sehr umfangreich und betreffen das Konzept sowie den gesamten Entwicklungs- und Herstellungsprozess. Solche Geräte werden deshalb speziell für Sicherheitsfunktionen konzipiert. Beispiele sind SIMATIC S7-300F / S7 400F/FH und SINUMERIK „Safety Integrated" sowie die Kommunikationssysteme PROFIsafe und ASIsafe, die Profibus und AS-Interface zur Übertragung sicherheitsbezogener Daten verwenden.

Sicherheitsbezogene Funktionen

Die sicherheitsbezogenen Funktionen umfassen neben den klassischen Funktionen

- Stillsetzen
- Handlungen im Notfall
- Verhindern unbeabsichtigten Anlaufs

inzwischen auch komplexere Funktionen wie

- Zustandsabhängige Verriegelungen
- Geschwindigkeitsbegrenzung
- Positionsbegrenzung
- Kontrolliertes Stillsetzen
- Kontrolliertes Halten u.ä.

Die klassischen Funktionen sind in EN 60204-1 definiert und wurden bisher im Allgemeinen durch einfache elektromechanische Bauteile realisiert. Sie können aber, ebenso wie komplexere Funktionen, auch durch programmierbare elektronische Systeme realisiert werden, wenn diese die relevanten Normen (IEC 61508, EN 954) erfüllen. Komplexe Funktionen, die z.B. das Verhalten drehzahlveränderbarer Antriebe betreffen, werden in draft IEC 61800-5-2 beschrieben.

Stillsetzen

Stop-Kategorien der EN 60204-1

Zum Stillsetzen einer Maschine sind in EN 60204-1 (VDE 0113 Teil 1) drei Stop-Kategorien definiert, die den Steuerablauf für das Stillsetzen unabhängig von einer Notfallsituation beschreiben:

Stop-Kategorie 0

Ungesteuertes Stillsetzen durch sofortige Abschaltung der Energie zu den Maschinenantriebselementen.

Stop-Kategorie 1

Gesteuertes Stillsetzen; Energiezufuhr wird erst dann unterbrochen, wenn Stillstand erreicht ist.

Stop-Kategorie 2

Gesteuertes Stillsetzen, bei dem die Energiezufuhr im Stillstand erhalten bleibt.
Hinweis: Durch das Abschalten wird nur die Zufuhr der Energie, die eine Bewegung verursachen kann, unterbrochen. Es wird nicht spannungsfrei geschaltet.

Handlung im Notfall

EN 60204-1/11.98 hat folgende mögliche Handlungen für Notfälle festgelegt und definiert (EN 60204-1 Anhang D). Die Begriffe in Klammern entsprechen der Ausführung im Schlussentwurf der Ausgabe 5.0 von IEC 60204-1).

Eine Handlung im Notfall schließt einzeln oder in Kombination ein:

- Stillsetzen im Notfall (Not-Halt);
- Ingangsetzen im Notfall (Not-Start);
- Ausschalten im Notfall (Not-Aus);
- Einschalten im Notfall (Not-Ein).

Diese Funktionen werden nach EN 60204-1 und nach EN 418 (Neufassung ISO 13850) ausschließlich durch eine bewusste menschliche Handlung ausgelöst. Im Folgenden wird nur auf das „Ausschalten im Notfall" und auf das „Stillsetzen im Notfall" weiter eingegangen. Letzteres entspricht voll dem gleichnamigen Begriff in der EU-Maschinenrichtlinie (engl. Emergency Stop). Der Einfachheit halber werden im Folgenden die alternativen Begriffe Not-Aus und Not-Halt verwendet.

Hinweis: In Deutschland wird für das „Stillsetzen im Notfall" neben dem Begriff Not-Halt häufig auch der Begriff Not-Aus verwendet, auch wenn damit nur das Stillsetzen gemeint ist.

Not-Aus

Eine Handlung im Notfall, die dazu bestimmt ist, die Versorgung mit elektrischer Energie zu einer ganzen oder zu einem Teil einer Installation abzuschalten, falls ein Risiko für elektrischen Schlag oder ein anderes Risiko elektrischen Ursprungs besteht (aus EN 60204-1 Anhang D).

Funktionale Aspekte zum Ausschalten im Notfall sind in IEC 60364-4-46 (identisch mit HD 384-4-46 und VDE 0100 Teil 460) festgelegt.

Ein Ausschalten im Notfall ist vorzusehen, wo

- Schutz gegen direktes Berühren (z.B. mit Schleifleitungen, Schleifringkörpern, Schaltgeräten in elektrischen Betriebsräumen) nur durch Abstand oder Hindernisse erreicht wird;
- es die Möglichkeit anderer Gefährdungen oder Beschädigungen durch elektrische Energie gibt.

Weiterhin heißt es in 9.2.5.4.3 von EN 60204-1:
Ein Ausschalten im Notfall wird durch Abschalten der Maschine von der Versorgung erreicht, mit der Folge eines Stops der Kategorie 0.

Wenn für eine Maschine der Stop der Kategorie 0 nicht zulässig ist, kann es notwendig sein, einen anderen Schutz z.B. gegen direktes Berühren vorzusehen, so dass ein Ausschalten im Notfall nicht notwendig ist.

Dies bedeutet, dass Not-Aus dort einzusetzen ist, wo die Risikoanalyse eine Gefährdung durch die elektrische Spannung / Energie ergibt und deshalb ein unverzügliches und umfassendes Abschalten der elektrischen Spannung erfordert.

Not-Aus-Einrichtungen fallen im Anwendungsbereich der EU unter die Niederspannungsrichtlinie 73/23/EWG, wenn sie nicht im Zusammenhang mit Maschinen eingesetzt werden.

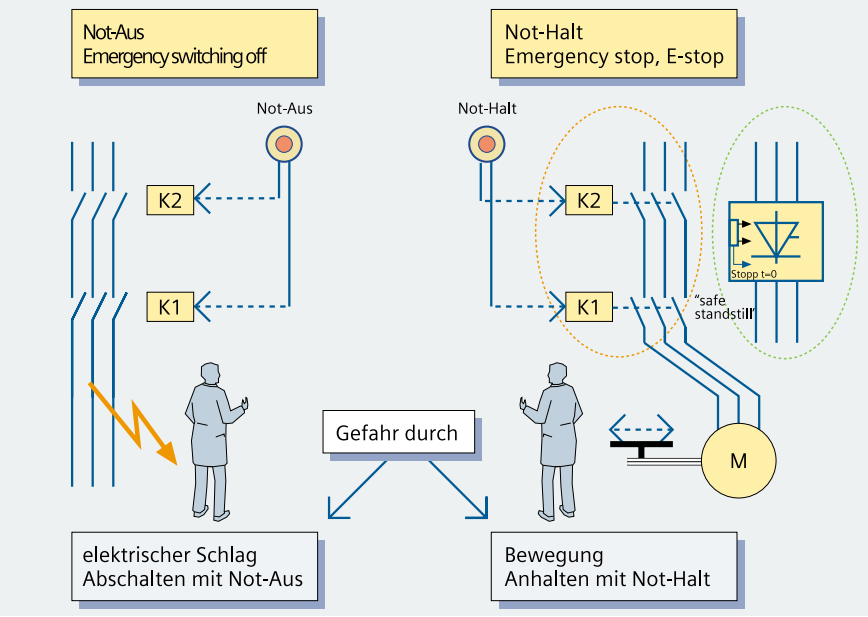


Bild 1/7
Unterscheidung Not-Aus – Not-Halt

Sofern sie im Zusammenhang mit Maschinen eingesetzt werden, fallen sie wie die gesamte andere elektrische Ausrüstung der Maschine auch unter die Maschinenrichtlinie 98/37/EG.

Not-Halt

Eine Handlung im Notfall, die dazu bestimmt ist, einen Prozess oder eine Bewegung anzuhalten, der (die) gefahrbringend wurde (aus EN 60204-1 Anhang D).
Weiterhin heißt es in 9.2.5.4.2 von EN 60204-1:

Stillsetzen

Zusätzlich zu den Anforderungen für Stop (siehe 9.2.5.3) gelten für das Stillsetzen im Notfall folgende Anforderungen:

- Es muss gegenüber allen anderen Funktionen und Betätigungen in allen Betriebsarten Vorrang haben;
- Die Energie zu den Maschinen-Antriebselementen, die einen gefahrbringenden Zustand bzw. gefahrbringende Zustände verursachen können, muss ohne Erzeugung anderer Gefährdungen so schnell wie möglich abgeschaltet werden (z.B. durch mechanische Anhaltevorrichtungen, die keine externe Versorgung erfordern, durch Gegenstrombremsen bei Stop-Kategorie 1);
- Das Rücksetzen darf keinen Wiederanlauf einleiten.

Das Stillsetzen im Notfall muss entweder als ein Stop der Kategorie 0 oder der Kategorie 1 wirken (siehe 9.2.2).

Die Kategorie für das Stillsetzen im Notfall muss anhand der Risikobeurteilung für die Maschine festgelegt werden.

Für die technische Realisierung des Not-Halt können, entsprechend der Anwendungsempfehlung im Vorwort von EN 60204-1, entweder die Anforderungen in EN 60204-1 oder in EN 954 und IEC 61508 angewendet werden. EN 60204-1 Ausgabe 4 fordert vorrangig die Realisierung durch elektromechanische Komponenten, da „einfache" (programmierbare) elektronische Systeme nicht sicher genug sind. Durch die richtige Anwendung von EN 954 und ggf. IEC 61508 werden elektronische und programmierbare elektronische Komponenten so funktionssicher, dass sie ebenfalls zur Realisierung des Not-Halt für alle Kategorien eingesetzt werden.

Mit der Ausgabe 5 (erwartet für 2005) werden die Anforderungen für die Not-Halt Funktion aktualisiert. Im Schlussentwurf von 2004 (die endgültige Fassung lag zum Zeitpunkt der Erstellung dieses Textes noch nicht vor) heißt es:

The emergency stop shall function either as a category 0 stop or as a category 1 stop (see 9.2.2). The choice of the category of the emergency stop depends on the results of a risk assessment of the machine.

In addition to the requirements for stop (see 9.2.5.3), the emergency stop function has the following requirements:

- *it shall override all other functions and operations in all modes;*
- *power to the machine actuators that can cause a hazardous condition(s) shall be either removed immediately (stop category 0) or shall be controlled in such a way to stop the hazardous motion as quickly as possible (stop category 1) without creating other hazards;*
- *reset shall not initiate a restart.*

Mit dieser neuen Formulierung entfällt die Einschränkung auf die Anwendung von festverdrahteten elektromechanischen Betriebsmitteln für die Realisierung von Sicherheitsfunktionen.

Geräte für Not-Aus und Not-Halt

Geräte für das Stillsetzen im Notfall müssen an jedem Bedienstand sowie an anderen Orten, wo die Einleitung eines Stillsetzens im Notfall erforderlich sein kann, vorhanden sein (Ausnahme: kabellose Bedienstationen).

Um die Schutzziele sowohl der EN 60204-1 als auch der EN 418 zu erfüllen, gelten für beide Funktionen folgende Anforderungen (s.a. 10.7 in EN 60204-1):

- Bei einem Schalten der Kontakte, auch bei einer nur kurzer Betätigung, muss das Befehlsgerät zwangsweise verrasten.
- Es darf nicht möglich sein, dass die Maschine von einem entfernten Hauptbedienstand wieder gestartet wird, ohne dass die Gefahr vorher beseitigt wurde. Die Notschalteinrichtung muss „vor Ort" durch eine bewusste Handlung wieder entriegelt werden.

Kabellose Bedienstationen müssen eine eigene und eindeutig erkennbare Möglichkeit haben, um die Stop-Funktion der Maschine einzuleiten. Das Bedienteil, das diese Stop-Funktion einleitet, darf nicht als Einrichtung zum Stillsetzen im Notfall markiert oder beschriftet sein.

Realisierung sicherheitsbezogener Funktionen

Bei der Realisierung sicherheitsbezogener Steuerungsfunktionen sind die Anforderungen von ISO 13849 (EN 954) bzw. IEC 62061 (IEC 61508) entsprechend der geforderten Risikominderung zu erfüllen. Mit Berücksichtigung der Anforderungen dieser Normen ist es möglich, auch komplexe Funktionen durch die Verwendung von Elektronik und programmierbarer Elektronik wie z.B. einer fehlersicheren SIMATIC oder SINUMERIK sicherheitsgerichtet zu realisieren.

Mensch – Maschine (Farbkennzeichnung für Bedienteile und Anzeigen)

Um das Zusammenwirken zwischen Mensch und Maschine zu erleichtern, werden in den Normen EN 60073 sowie DIN EN 60204 Vorgaben zur Kennzeichnung und Codierung gemacht.

Zu den Maschinenkomponenten, die im Schnittstellenbereich Mensch – Maschine eingesetzt werden, zählen in erster Linie Schalter, Taster und Leuchtmelder. Die durchgängige eindeutige Kennzeichnung dieser Bedienelemente erfolgt durch farbliche Kennzeichnung, die einer konkreten Bedeutung zugeordnet sind. Dadurch ist gewährleistet, dass die Sicherheit des Bedienpersonals erhöht und die Bedienung und Wartung der Betriebsmittel/Anlagen erleichtert werden.

Die Farben für Drucktaster, die Bedeutung der Farben sowie Erklärungen und Anwendungsbeispiele werden in Bild 1/8 angegeben.
Gemäß DIN EN 60204-1 (VDE 0113 Teil 1) sind folgende Hinweise zu beachten:

Die bevorzugten Farben für START/EIN-Bedienteile sollten WEISS, GRAU oder SCHWARZ, vorzugsweise WEISS sein. GRÜN darf, ROT darf nicht verwendet werden.

Die Farbe ROT muss für Not-Aus- und Not-Halt-Bedienteile verwendet werden.

Die Farben für STOP/AUS-Bedienteile sollten SCHWARZ, GRAU oder WEISS, vorzugsweise SCHWARZ sein. ROT ist ebenfalls erlaubt. GRÜN darf nicht benutzt werden.

WEISS, GRAU und SCHWARZ sind die bevorzugten Farben für Drucktaster-Bedienteile, die wechselweise als START/EIN- und STOP/AUS-Drucktaster wirken. Die Farben ROT, GELB oder GRÜN dürfen nicht verwendet werden.

WEISS, GRAU und SCHWARZ sind die bevorzugten Farben für Drucktaster-Bedienteile, die einen Arbeitsvorgang bewirken, während sie betätigt sind und den Betrieb beenden, wenn sie losgelassen werden (z.B. Tippen).

Die Farben ROT, GELB und GRÜN dürfen nicht verwendet werden.

Die Farbe GRÜN ist für Funktionen reserviert, die einen sicheren oder normalen Zustand anzeigen.

Die Farbe GELB ist für Funktionen reserviert, die eine Warnung oder einen anormalen Zustand anzeigen.

Die Farbe BLAU ist für Funktionen von zwingender Bedeutung reserviert.

Rückstell-Drucktaster müssen BLAU, WEISS, GRAU oder SCHWARZ sein. Falls sie auch als STOP/AUS-Taster wirken, werden die Farben WEISS, GRAU oder SCHWARZ bevorzugt, vorzugsweise SCHWARZ. GRÜN darf nicht benutzt werden.

Wenn dieselbe Farbe Weiß, Grau oder Schwarz für verschiedene Funktionen verwendet wird (z.B. Weiß für Starter/Ein und Stop/Aus Betätiger), müssen zusätzliche Mittel der Codierung (z.B. in Form, Position, Symbol) zur Identifikation verwendet werden.

In Bild 1/9 werden die Farben für Leuchtmelder, ihre Bedeutung in Bezug auf den Zustand der Maschine sowie Handhabung und Anwendungsbeispiele aufgeführt.

Bei Leuchtdrucktastern gelten ebenfalls die Bilder 1/8 und 1/9.
Bei Problemen mit der Zuordnung geeigneter Farben muss auf die Farbe WEISS zurückgegriffen werden. Für Not-Aus-Geräte darf die Farbe ROT nicht von der Beleuchtung abhängen.

Farbe	Bedeutung	Erklärung	Anwendungsbeispiele
ROT	Notfall	Bei gefährlichem Zustand oder im Notfall betätigen	NOT-AUS, Einleitung von NOT-AUS-Funktionen, bedingt für STOP/AUS
GELB	Anormal	Bei anormalem Zustand betätigen	Eingriff, um anormalen Zustand zu unterdrücken, Eingriff, um einen unterbrochenen automatischen Ablauf wieder zu starten
GRÜN	Sicher	Bei sicherer Bedingung betätigen oder im normalen Zustand vorzubereiten	START/EIN, hierfür jedoch bevorzugt WEISS
BLAU	Zwingend	Bei Zustand betätigen, der zwingende Handlung erfordert	Rückstellfunktion
WEISS	Keine spezielle Bedeutung zugeordnet	Für allgemeine Einleitung von Funktionen außer NOT-AUS (siehe auch Anmerkung)	START/EIN (bevorzugt), STOP/AUS
GRAU			START/EIN, STOP/AUS
SCHWARZ			START/EIN, STOP/AUS (bevorzugt)

Anmerkung: Wird eine zusätzliche Maßnahme der Kennzeichnung (z. B. Struktur, Form, Lage) zum Kennzeichnen von Drucktaster-Bedienteilen verwendet, dürfen dieselben Farben WEISS, GRAU oder SCHWARZ für verschiedene Funktionen verwendet werden, z. B. WEISS für START/EIN- und STOP/AUS-Bedienteile.

Bild 1/8
Farben für Drucktaster und ihre Bedeutung nach EN 60204-1 (VDE 0113 Teil 1): 06.93

Farbe	Bedeutung	Erklärung	Handlung durch den Bediener	Anwendungsbeispiele
ROT	Notfall	Gefährlicher Zustand	Sofortige Handlung, um auf gefährlichen Zustand zu reagieren (z. B. durch Betätigung des NOT-AUS)	Druck/Temperatur außerhalb sicherer Grenzen, Spannungsfall, Spannungszusammenbruch, Überfahren einer Stop-Position
GELB	Anormal	Anormaler Zustand Bevorstehender kritischer Zustand	Überwachen und/oder Eingreifen (z. B. durch Wiederherstellen der beabsichtigten Funktion)	Druck/Temperatur übersteigt normale Bereiche, Auslösen einer Schutzeinrichtung
GRÜN	Normal	Normaler Zustand	Optional	Druck/Temperatur innerhalb normaler Bereiche, Ermächtigung fortzufahren
BLAU	Zwingend	Anzeige eines Zustandes, der Handlung durch den Bediener erfordert	Zwingende Handlung	Anweisung, vorgegebene Werte einzugeben
WEISS	Neutral	Andere Zustände: darf verwendet werden, wenn Zweifel über die Anwendung von ROT, GELB, GRÜN oder BLAU bestehen	Überwachen	Allgemeine Informationen

Bild 1/9
Farben für Leuchtmelder und ihre Bedeutung nach EN 60204-1 (VDE 0113 Teil 1): 06.93

Kennzeichnung von Leitungen

Im vorangegangenen Kapitel ist die farbige Codierung von Schaltern, Tastern und Leuchtmeldern behandelt worden. Bei der Kennzeichnung von Leitern sind durch die Norm EN 60204 größere Spielräume erlaubt. Sie schreibt nämlich vor, dass die „... Leiter an jeden Anschluss in Übereinstimmung mit der technischen Dokumentation identifizierbar sein müssen ...".

Die Nummerierung von Klemmen in Übereinstimmung mit dem Schaltplan genügt, wenn die Leitung visuell leicht verfolgbar ist. Bei umfangreichen Steuerungen empfiehlt es sich, sowohl den Leiter der Innenverdrahtung als auch den nach außen abgehenden Leiter so zu kennzeichnen, dass man nach dem Lösen später den Draht wieder an die richtige Klemme bringen kann. Es ist auch dort zu empfehlen, wo die Leiter für den Transport aufgetrennt werden müssen.

Mit der Formulierung in IEC 60204-1 1997, Absatz 14.2.1 Aderkennzeichnung, wollte das Normenkomitee folgende Punkte zum Ausdruck bringen:

1. Jeder einzelne Leiter muss identifizierbar sein, jedoch in dieser Absolutheit nur im Zusammenhang mit der Dokumentation. Es ist nicht gefordert, dass jeder Leiter für sich, ohne Dokumentation identifizierbar sein muss.

2. Die Art der Kennzeichnung und damit auch die Identifizierungsmethode sollte gegebenenfalls zwischen Hersteller und Betreiber vereinbart werden.

Es ist nicht Absicht der Norm, eine bestimmte Kennzeichnungsart zwingend weltweit vorzuschreiben. Aus Sicherheitsgründen können z.B. werksinterne Festlegungen eine höhere Priorität haben, um in Bereichen, die von demselben Personal betreut werden, Verwechslungen vorzubeugen. Diese Festlegungen können wegen des großen Geltungsbereiches der vorliegenden Norm von kleinen Einzelmaschinen (Massenprodukte) bis zu großen komplexen maschinellen Anlagen (Unikate) nicht verallgemeinert werden.

Primär muss die Sicherheit vor Montagefehlern durch entsprechende Prüfungen sichergestellt sein.

Es soll eine einheitliche Farbkennzeichnung der Leitungen verwendet werden. Folgende Farbzuordnung wird empfohlen:

- Schwarz für Hauptstromkreise für Wechsel- und Gleichstrom
- Rot für Steuerstromkreise für Wechselstrom
- Blau für Steuerstromkreise für Gleichstrom
- Orange für Verriegelungsstromkreise, die von einer externen Stromquelle versorgt werden.

Entschließt man sich zu einer reinen Farbkennzeichnung, so wird die obige Farbzuordnung empfohlen. Bindend vorgeschrieben ist lediglich die Farbe von Schutzleiter und Neutralleiter. Für alle anderen Leiter kann frei zwischen den in 14.2.4 aufgelisteten Methoden gewählt werden (Farbe, Ziffern oder Buchstaben; oder eine Kombination aus Farbe und Ziffern oder Farbe und Buchstaben).

Kennzeichnung des Schutzleiters

Der Schutzleiter muss durch Form, Anordnung, Kennzeichnung oder Farbe deutlich zu erkennen sein. Wenn Kennzeichnung nur durch Farbe erfolgt, dann muss es die Zweifarben-Kombination Grün/Gelb sein, die sich über die gesamte Leiterlänge erstrecken muss. Die Farbkennzeichnung Grün/Gelb ist ausschließlich dem Schutzleiter vorbehalten.

Kennzeichnung des Neutralleiters

Enthält ein Stromkreis einen farblich gekennzeichneten Neutralleiter, muss die Farbe Hellblau verwendet werden. Hellblau darf nicht zur Kennzeichnung von anderen Leitern verwendet werden, wenn die Gefahr der Verwechslung besteht.

Fehlt ein Neutralleiter, darf ein hellblauer Leiter für andere Zwecke verwendet werden, aber nicht als Schutzleiter.

Prozesstechnik in Europa

Gesetzliche Anforderungen in Europa

In der Prozesstechnik sind im Wesentlichen die folgenden EU-Richtlinien anzuwenden:

- Richtlinie 96/82/EG des Rates vom 9. Dez. 96 zur Beherrschung der Gefahren bei schweren Unfällen mit gefährlichen Stoffen („Seveso-Richtlinie" II).
- Niederspannungsrichtlinie
- Maschinenrichtlinie (98/37/EG)
- Druckgeräterichtlinie (97/23/EG). Sie ist nur insofern relevant, als die verwendeten Geräte diese Richtlinie erfüllen müssen. „Die Richtlinie gilt dagegen nicht für den Zusammenbau von Druckgeräten, der auf dem Gelände des Anwenders, beispielsweise in Industrieanlagen, unter seiner Verantwortung erfolgt."

Parallel dazu müssen immer die Arbeitsschutzgesetze und Unfallverhütungsvorschriften beachtet werden. (In Deutschland „Betriebssicherheitsverordnung" (BetrSichV).)

„Seveso-Richtlinie"

Wichtiger Bestandteil dieser EU-Richtlinie ist die Verpflichtung der Unternehmen, ein Sicherheitsmanagementsystem einzurichten, das eine gründliche Risikoabschätzung unter Verwendung der möglichen Unfallszenarien einschließt. Sie nennt, entsprechend den in der Einleitung erläuterten Prinzipien, das Sicherheitsziel,

⇒ durch vorbeugende Maßnahmen die Qualität der Umwelt zu erhalten und die Gesundheit des Menschen zu schützen."

Zur Erreichung dieses Zieles werden folgende grundlegende Forderungen erhoben, für deren Erfüllung die Mitgliedsstaaten sorgen müssen.

⇒ Konzept zur Verhütung schwerer Unfälle

Der Betreiber ist verpflichtet, „... eine Unterlage zur Verhütung schwerer Unfälle auszuarbeiten und deren ordnungsgemäße Umsetzung sicherzustellen. Mit dem vom Betreiber vorgesehenen Konzept zur Verhütung schwerer Unfälle soll durch geeignete Mittel, Organisation und Managementsysteme ein hohes Schutzniveau für Mensch und Umwelt sichergestellt werden" (Artikel 7 Absatz 1).

Die Unterlage muss u.a. folgende Grundsätze berücksichtigen:

- Das Konzept zur Verhütung schwerer Unfälle ist schriftlich auszufertigen.
- Ein Sicherheitsmanagementsystem, in dem u.a. folgende Punkte geregelt werden:
  - Ermittlung und Bewertung der Risiken – Festlegung und Anwendung von Verfahren zur systematischen Ermittlung der Risiken.
  - Betriebskontrolle – Festlegung und Anwendung von Verfahren für den sicheren Betrieb, einschließlich der Wartung der Anlagen.
  - Qualitätssicherung – Festlegung und Anwendung von Verfahren zur ständigen Bewertung der Erreichung der Ziele.

⇒ Sicherheitsbericht

Der Betreiber ist verpflichtet, einen Sicherheitsbericht zu erstellen, in dem dargelegt wird,

- dass ein Konzept ... umgesetzt wurde,
- dass die Gefahren ermittelt und alle erforderlichen Maßnahmen zur Verhütung derartiger Unfälle und Begrenzung der Folgen für Mensch und Umwelt ergriffen wurden und
- dass die Auslegung, die Errichtung sowie der Betrieb sämtlicher Anlagen, ... ausreichend sicher und zuverlässig sind.

⇒ Inspektion

Die Behörden haben ein System von Inspektionen zur systematischen Prüfung der betriebstechnischen, organisatorischen und managementspezifischen Systeme des Betriebs einzurichten, mit dem sich die Behörde vergewissert, dass der Betreiber nachweisen kann,

- dass er die zur Verhütung schwerer Unfälle erforderlichen Maßnahmen ergriffen hat und
- dass er angemessene Mittel zur Begrenzung der Folgen ... vorgesehen hat.

Die Erfüllung dieser EU-Richtlinie muss national umgesetzt werden. In Deutschland erfolgt das durch die Störfallverordnung.

Hinweis: Die „Seveso-Richtlinie" ist keine Richtlinie des „New Approach", d.h. das Prinzip, dass bei der Anwendung harmonisierter Normen automatisch vermutet werden darf, dass die Ziele der Richtlinie erfüllt sind, gilt hier nicht. Die genauen Anforderungen sind national geregelt.

Deutsche Ausführungsbestimmung:
⇒ **Störfallverordnung**

Mit der Störfallverordnung wird die „Seveso-Richtlinie"in Deutschland im Sinne des Gesetzgebers umgesetzt. Sie legt u.a. fest, auf welche Anlagen die EU-Richtlinie anzuwenden ist.

Anlagen, die der Störfallverordnung unterliegen, müssen nach Neubau oder signifikanten Änderungen vom Gewerbeaufsichtsamt vor der Inbetriebnahme dahingehend geprüft werden, ob sie dem Stand der Technik zur Erfüllung der Sicherheitsziele entsprechen. Die Beurteilung erfolgt auf der Basis der relevanten Normen.

Technische Maßnahmen zur Erfüllung der gesetzlichen Ziele

An erster Stelle steht immer das Ziel, den Prozess so zu gestalten, dass er in sich sicher ist. Wo das nicht in ausreichendem Umfang möglich ist, sind zusätzliche Maßnahmen erforderlich, um das verbliebene Risiko, das von dem Prozess ausgeht, auf eine akzeptable Größe zu reduzieren. Dies kann mit Mitteln der Prozessleittechnik (PLT) erfolgen, wenn diese für die besondere Aufgabe geeignet sind. PLT-Maßnahmen und -Einrichtungen sind dann für Aufgaben der Anlagensicherung geeignet, wenn sie speziell dafür ausgelegt sind. Die Anforderungen dafür sind in Normen beschrieben.

Relevante Normen für Sicherungsmaßnahmen mit Mitteln der Prozessleittechnik

Für Sicherungsmaßnahmen mit Mitteln der Prozessleittechnik werden in Deutschland bisher die folgenden nationalen Normen angewendet:

Nach der europäischen Ratifizierung von IEC 61508 als EN 61508 haben die nationalen Normen DIN V 19250 und 19251 in 08.2004 ihre Gültigkeit verloren und es ist statt dessen EN 61508 anzuwenden. Als spezifische Norm für die Prozessindustrie steht IEC 61511 „Functional safety: safety instrumented systems for the process industry sector" zur Verfügung. Sie beschreibt die Anforderungen von EN/IEC 61508 spezifisch für die Prozessindustrie. Eine Ratifizierung als EN 61511 ist Ende 2004 zu erwarten.

Für die eingesetzten Geräte und Einrichtungen gelten darüber hinaus weitere Normen, die sich mit deren spezifischen Sicherheitsanforderungen befassen. Siehe dazu Kapitel Maschinensicherheit (siehe Kapitel 1.2).

Anwenderrichtlinien

Für die praktische Ausführung der Anlagensicherung gibt es in Deutschland eine Richtlinie VDI/VDE 2180 „Sicherung von Anlagen der Verfahrenstechnik mit Mitteln der Prozessleittechnik", in der die Anforderungen der relevanten Norm in vereinfachter Form beschreiben sind. Die Neufassung der VDI/VDE 2180 berücksichtigt IEC 61511 und beinhaltet auch die Anforderungen von NE 31 „Anlagensicherung mit Mitteln der Prozessleittechnik" und NE 79: „Mikroprozessorbestückte Geräte in der Anlagensicherung".

Dieses Dokument dient als praktischer Leitfaden. Hinsichtlich der Auswahl von Sicherheits-SPS und anderer mikroprozessorbasierter Komponenten (z.B. Transmitter) bieten die oben genannten Normen eine differenziertere Betrachtung als die Anwenderrichtlinien und sollten bei Bedarf mit beachtet werden.

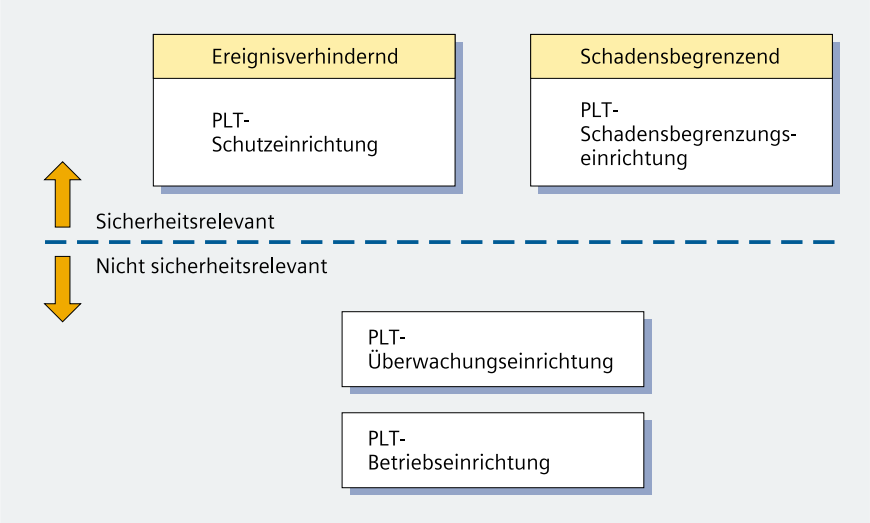


Bild 1/10
Einordnung von PLT-Einrichtungen in sicherheitsrelevant / nicht sicherheitsrelevant

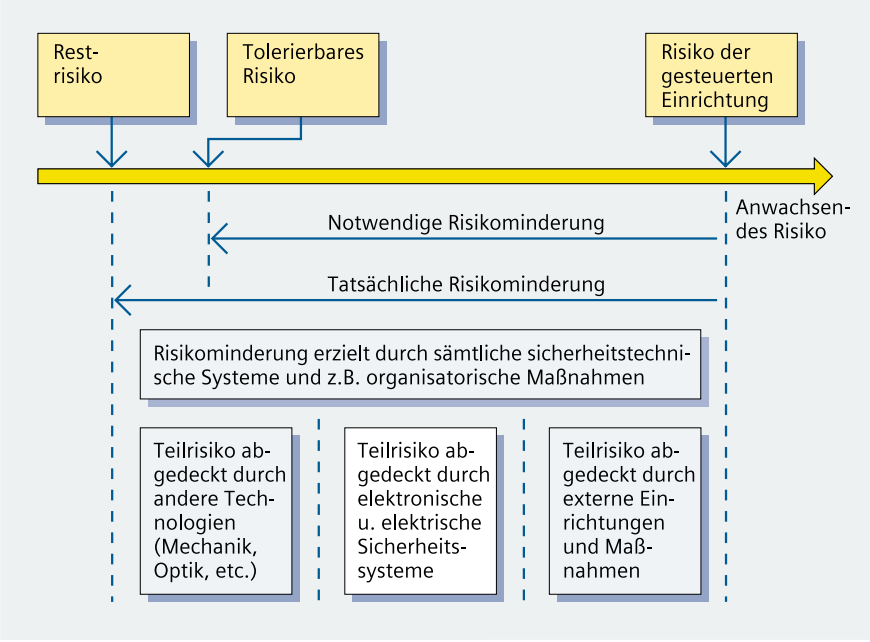


Bild 1/11
Prinzip der Risikoreduzierung (gem. IEC 61508)

Risikominderung mit Mitteln der Prozessleittechnik (PLT)

Maßnahmen zur Risikominderung sind dann notwendig, wenn Fehler oder Störungen in den PLT-Betriebs- und Überwachungseinrichtungen zu einem gefährlichen Ereignis oder gefährlichen Zustand der Anlage führen können und wenn das daraus resultierende Risiko unakzeptabel hoch ist. In diesem Fall ist es notwendig, durch geeignete Schutzmaßnahmen entweder die Wahrscheinlichkeit für das Eintreten des gefährlichen Ereignisses ausreichend zu verringern oder das Schadensausmaß zu verkleinern. Das kann durch PLT-Schutzeinrichtungen erfolgen, wenn diese die Sicherheitsanforderungen erfüllen.

Risikoreduzierung

Da ein vollständiger Ausschluss bestimmter Risiken technisch und wirtschaftlich nicht möglich ist, ist es notwendig, nicht nur das vorhandene Risiko zu ermitteln, sondern auch das tolerierbare Risiko festzulegen. Aus der Differenz zwischen beiden leitet sich dann das Maß für die sicherheitsbezogene Zuverlässigkeit („safety integrity“) der risikoreduzierenden Funktionen ab. EN 61508 definiert „Safety Integrity Level“ (SIL) als Zielmaß für die Versagenswahrscheinlichkeit für die Ausführung der risikoreduzierenden Funktionen. Für Sicherheitstechnische Systeme der Prozessindustrie, die im Anforderungsmodus arbeiten, ist dieses Maß in IEC 61511 als Risikominderungsfaktor definiert.

Safety Integrity level	Betrieb im häufigen Anforderungs- oder kontinuierlichen Modus (Wahrscheinlichkeit eines gefährlichen Ausfalls pro Stunde)	Betrieb im geringen Anforderungsmodus (Mittlere Wahrscheinlichkeit des Versagens der vorgesehenen Funktion bei Anforderung)
4	$\geq 10^{-9}$ bis $< 10^{-8}$	$\geq 10^{-5}$ bis $< 10^{-4}$
3	$\geq 10^{-8}$ bis $< 10^{-7}$	$\geq 10^{-4}$ bis $< 10^{-3}$
2	$\geq 10^{-7}$ bis $< 10^{-6}$	$\geq 10^{-3}$ bis $< 10^{-2}$
1	$\geq 10^{-6}$ bis $< 10^{-5}$	$\geq 10^{-2}$ bis $< 10^{-1}$

Bild 1/12
Safety integrity levels gemäß IEC 61508: Zielmaß der Versagenswahrscheinlichkeit einer Sicherheitsfunktion, die einem sicherheitsrelevanten System zugeordnet ist

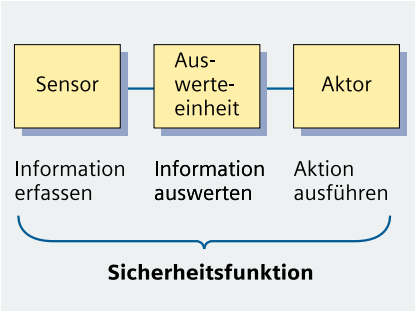


Bild 1/13
Auswerteeinheit, z.B. Sicherheits-SPS

Auswahl der Geräte und Grundlagen der geforderten Eigenschaften

Sicherheitsfunktion

Risikominderung mit Mitteln der PLT erfolgt dadurch, dass für jedes mögliche gefährliche Ereignis oder jeden möglichen gefährlichen Zustand einer Anlage Funktionen definiert werden, die das Eintreten des gefährlichen Ereignisses verhindern. Diese so genannten „Sicherheitsfunktionen" dienen dazu, einen sicheren Zustand der Anlage zu erhalten bzw. wieder herzustellen, wenn aufgrund eines Fehlers oder einer Störung in der Anlage ein gefährliches Ereignis einzutreten droht. Die Sicherheitsfunktion kann auch dazu dienen, das Ausmaß des Schadens aufgrund eines gefährlichen Ereignisses zu verringern.

Die Definition einer Sicherheitsfunktion umfasst immer die Spezifikation der Funktion selbst (z.B. Sperren des Zuflusses zu einem Behälter, wenn der Füllstand die Höchstgrenze erreicht hat) und die aus der Risikoanalyse abgeleitete „Safety Integrity (SIL)".

Realisierung der Sicherheitsfunktionen

Jede Sicherheitsfunktion umfasst immer die ganze Kette, von der Informationserfassung über die Informationsauswertung bis hin zur Durchführung der beabsichtigten Aktion.

Die daran beteiligten Geräte wie z.B. fehlersichere SPS, Sensoren und Aktoren usw. müssen in ihrer Gesamtheit den bei der Risikobewertung ermittelten SIL erfüllen. Wird ein Gerät zugleich für verschiedene Sicherheitsfunktionen verwendet, hat es den höchsten SIL der einzelnen Funktionen zu erfüllen.

Geräteeigenschaften

Werden für die Informationsverarbeitung SPS eingesetzt, müssen diese als „Sicherheits-SPS" (SSPS) die Anforderungen der relevanten Normen (z.B. IEC 61508), entsprechend dem angegebenen SIL, erfüllen und sollten von einem unabhängigen Prüfer zertifiziert sein. Die wesentlichen Eigenschaften einer fehlersicheren SPS, die in den Normen in abgestuftem Umfang gefordert werden, sind:

- Bei Entwicklung, Herstellung und Wartung sind bestimmte Maßnahmen und Verfahren anzuwenden, damit systematische Fehler vermieden werden.
- Die SPS muss in der Lage sein, systematische Fehler, die während des Betriebes wirksam werden, zu beherrschen.
- Die SPS muss zufällige Hardwareausfälle während des Betriebes erkennen und beherrschen können.
- Fehlerbeherrschung bedeutet, dass das System bei Erkennen eines Fehlers so reagiert, dass eine für diesen Fall festgelegte Sicherheitsfunktion (z.B. Abschalten der Anlage) zuverlässig ausgeführt wird.

Ähnliche Anforderungen gelten auch für komplexe Feldgeräte. Details dazu beschreibt IEC 61511.

Anwendung

Bei der Anwendung einer fehlersicheren SPS müssen die in dem zugehörigen Sicherheitshandbuch festgelegten Bedingungen und ggf. zusätzliche Auflagen des Zertifikates eingehalten werden.

Für die anzuschließenden Peripheriegeräte (z.B. Sensoren und Aktoren) sind zusätzlich die Anforderungen in den Normen (IEC 61508 bzw. IEC 61511) hinsichtlich folgender Aspekte zu beachten:

- Vermeiden systematischer Fehler wie z.B. Projektierungs-, Montage- und Handhabungsfehler.
- Aufdecken und Beherrschen zufälliger Fehler (Ausfälle).
- Notwendige Fehlertoleranz. Diese ist abhängig von dem Anteil der Ausfälle, die in eine sichere Richtung gehen.
- Erforderliche Wartung (wiederkehrende Prüfung).

IEC 61511 begrenzt den maximal zulässigen SIL, für den Feldgeräte eingesetzt werden dürfen, abhängig von deren Fehlertoleranz. Die in Bild 1/14 angegebene Fehlertoleranz kann um 1 vermindert werden, wenn:

- die Geräte betriebsbewährt sind,
- die Geräte nur die Einstellung prozessbezogener Parameter ermöglichen und
- die Einstellung der prozessbezogenen Parameter geschützt ist.

Um bei bestimmten Anwendungen die für deren SIL notwendige höhere Hardware-Fehlertoleranz zu erreichen, können Feldgeräte redundant betrieben werden, sofern die Geräte aufgrund ihrer übrigen Eigenschaften für diesen SIL geeignet sind.

Um Fehler in den Peripheriegeräten aufzudecken, können in der SPS Test- und Überwachungsfunktionen integriert werden. Eine ggf. erforderliche Reaktion muss dabei innerhalb einer ausreichend kurzen Zeit erfolgen.

Diese Zeitanforderungen sind abhängig von der Fehlertoleranz. Die genauen Anforderungen sind IEC 61511 definiert.

Bei der Anwendung komplexer Peripheriegeräte (z.B. Transmitter mit Mikroprozessor) ist darauf zu achten, dass diese Geräte selbst die relevanten Normen (EN 61508 bzw. IEC 61511) erfüllen.

Die gesamte PLT-Schutzeinrichtung ist so zu gestalten, dass sie für alle sicherheitsrelevanten Funktionen die gültigen Normen erfüllt. Bezüglich funktionaler Sicherheit sind das EN 61508 bzw. IEC 61511.

SIL	Mindest-Hardware-Fehlertoleranz, wenn die Hauptausfallrichtung in den sicheren Zustand gerichtet ist
1	0
2	1
3	2

Hinweis: Als „sicher" werden solche Ausfälle bezeichnet, bei denen ein sicherer Anlagenzustand erhalten bleibt.
Hinweis: Eine Fehlertoleranz von N bedeutet, dass N+1 Fehler zum Versagen der Funktion führen.

Bild 1/14
Maximal zulässiger SIL für Feldgeräte, abhängig von deren Fehlertoleranz (gemäß IEC 61511-1)

Feuerungsanlagen in Europa

EU-Richtlinien

Feuerungsanlagen und Brenner unterliegen den aufgrund ihres Einsatzes und der verwendeten Geräte relevanten Richtlinien (z.B. Maschinenrichtlinie, Druckgeräterichtlinie (...), Richtlinie für Gasbrenner (90/396/EEC)). Spezifische EU-Richtlinien für Feuerungsanlagen gibt es nicht. Sie unterliegen gegebenenfalls anwendungsspezifischen Richtlinien. Industrielle Thermoprozessanlagen sind z.B. als Maschinen unter der Maschinenrichtlinie eingeordnet.

Normen

Industrielle Thermoprozessanlagen

Für diese Anlagen gibt es europäische Normen der Reihe EN 746-x „Industrielle Thermoprozessanlagen...", die unter der Maschinenrichtlinie harmonisiert sind.

Die EN 746 ist anwendbar auf industrielle Thermoprozessanlagen u.a. in

- Metall erzeugenden und verarbeitenden Werken,
- Glashüttenwerken,
- Keramikwerken,
- Zement-, Kalk- und Gipswerken,
- Chemiewerken,
- Abfallverbrennungsanlagen usw.

Teil 1: „Allgemeine Sicherheitsanforderungen an industrielle Thermoprozessanlagen" verweist für die Realisierung der elektrischen Einrichtung auf EN 60204-1 und EN 954-1.

Feuerungsanlagen

Für Feuerungsanlagen, die nicht zu den industriellen Thermoprozessanlagen gehören und nicht zum Heizen von Prozessflüssigkeiten und -gasen in der chemischen Industrie verwendet werden, gibt es als allgemeine Normen für die elektrische Ausrüstung die europäische Norm

- EN 50156 „Electrical equipment for furnaces Part 1: Requirements for application design and installation"

Sie ersetzt die deutsche Norm DIN VDE 0116 „Elektrische Ausrüstung von Feuerungsanlagen". EN 50156 verlangt die Einhaltung von EN 60204-1. Die Anforderungen für sicherheitsrelevante Systeme basieren auf IEC 61508.

Als spezifische Normen für Brenner existieren zurzeit

- EN 676 Gasbrenner;
- EN 230 Ölzerstäubungsbrenner in Monoblockausführung;
- EN 267 Ölbrenner;
- EN 298 Feuerungsautomaten für Gasbrenner und Gasgeräte mit und ohne Gebläse.

1.3 Gesetzliche Anforderungen und Standard zur Sicherheit am Arbeitsplatz in Nordamerika

Hinweis: *Die folgende Beschreibung soll einen Überblick über die Prinzipien und grundlegenden Anforderungen vermitteln. Sie darf nicht als vollständige Beschreibung betrachtet werden. Der Leser muss sich zusätzlich über die genauen Anforderungen sowie nationalen und lokalen Regeln für seine spezielle Anwendung informieren.*

Ein wesentlicher Unterschied bei den gesetzlichen Anforderungen zur Sicherheit am Arbeitsplatz zwischen Nordamerika und Europa ist, dass es in Amerika keine einheitliche Bundesgesetzgebung zur Maschinensicherheit gibt, welche die Verantwortlichkeit des Herstellers/Lieferers abdeckt. Vielmehr besteht die generelle Anforderung, dass der Arbeitgeber einen sicheren Arbeitsplatz bieten muss.

USA allgemein

Die Anforderung, dass der Arbeitgeber einen sicheren Arbeitsplatz bieten muss, ist mit dem Occupational Safety and Health Act (OSHA) von 1970 geregelt. Die Kernanforderung des OSHA steht in Abschnitt 5 "Duties":

(a) Each employer -
(1) shall furnish to each of his employees employment and a place of employment which are free from recognized hazards that are causing or are likely to cause death or serious physical harm to his employees;
(2) shall comply with occupational safety and health standards promulgated under this Act.

Die Anforderungen aus dem OSH Act werden durch die Occupational Safety and Health Administration (ebenfalls als OSHA bezeichnet) verwaltet. OSHA setzt regionale Inspektoren ein, die prüfen, ob die Arbeitsplätze die gültigen Regeln erfüllen.

Die für Arbeitssicherheit relevanten Regeln der OSHA sind in OSHA 29 CFR 1910.xxx ("OSHA Regulations (29 CFR) PART 1910 Occupational Safety and Health") beschrieben. (CFR: Code of Federal Regulations).

Siehe www.osha.gov .

In den Regeln für das Safety and Health Programm (29 CFR 1900.1) heißt es am Anfang:

"(b)(1) What are the employer's basic obligations under the rule? Each employer must set up a safety and health program to manage workplace safety and health to reduce injuries, illnesses and fatalities by systematically achieving compliance with OSHA standards and the General Duty Clause."

Und später

"(e) Hazard prevention and control.

(e)(1) What is the employer's basic obligation? The employer's basic obligation is to systematically comply with the hazard prevention and control requirements of the General Duty Clause and OSHA standards.

(e)(2) If it is not possible for the employer to comply immediately, what must the employer do? The employer must develop a plan for coming into compliance as promptly as possible, which includes setting priorities and deadlines and tracking progress in controlling hazards. Note: Any hazard identified by the employer's hazard identification and assessment process that is covered by an OSHA standard or the General Duty Clause must be controlled as required by that standard or that clause, as appropriate."

Die Anwendung der Standards ist in 29 CFR 1910.5 "Applicability of standards" geregelt. Das Konzept ist ähnlich wie in Europa. Produktspezifische Standards haben Vorrang vor allgemeinen Standards, sofern die betreffenden Aspekte dort behandelt sind. Bei Erfüllung der Standards kann der Arbeitgeber annehmen, dass er die Kernforderung des OSH Act bezüglich der durch die Standards behandelten Aspekte erfüllt hat.

1910.5 (f) "An employer who is in compliance with any standard in this part shall be deemed to be in compliance with the requirement of section 5(a)(1) of the Act, but only to the extent of the condition, practice, means, method, operation, or process covered by the standard."

Maschinensicherheit

Mindestanforderungen der OSHA

Die OSHA Regeln unter 29 CFR 1910 enthalten allgemeine Anforderungen für Maschinen (1910.121) und eine Reihe spezifischer Anorderungen für bestimmte Maschinentypen. Die Anforderungen darin sind sehr spezifisch aber technisch wenig detailliert.
Zitat aus 29 CFR 1910.212 "General requirements for all machines":

"(a)(1)

Types of guarding. One or more methods of machine guarding shall be provided to protect the operator and other employees in the machine area from hazards such as those created by point of operation, ingoing nip points, rotating parts, flying chips and sparks. Examples of guarding methods arebarrier guards, two-hand tripping devices, electronic safety devices, etc."
Ein Beispiel für die Anforderungen an die Steuerung von Pressen ist das folgende Zitat aus 29 CFR 1910.217 "Mechanical Power Presses":

"(b)(13)

Control reliability. When required by paragraph (c)(5) of this section, the control system shall be constructed so that a failure within the system does not prevent the normal stopping action from being applied to the press when required, but does prevent initiation of a successive stroke until the failure is corrected. The failure shall be detectable by a simple test, or indicated by the control system. This requirement does not apply to those elements of the control system which have no effect on the protection against point of operation injuries."

"(h)(6)(xvii)

Controls with internally stored programs (e.g., mechanical, electro-mechanical, or electronic) shall meet the requirements of paragraph (b)(13) of this section, and shall default to a predetermined safe condition in the event of any single failure within the system. Programmable controllers which meet the requirements for controls with internally stored programs stated above shall be permitted only if all logic elements affecting the safety system and point of operation safety are internally stored and protected in such a manner that they cannot be altered or manipulated by the user to an unsafe condition."

Die OSHA Regeln beschreiben Mindestanforderungen zur Gewährleistung sicherer Arbeitsplätze. Sie sollen aber Arbeitgeber nicht daran hindern, neue innovative Methoden, z.B. "state of the art" Schutzsysteme anzuwenden, um die Sicherheit der Arbeitnehmer zu maximieren
(Siehe z.B.: www.osha.gov/ ...Standard Interpretations ... 06/05/2001 - Use of Electro Sensitive Protection Equipment ...)

OSHA verlangt im Zusammenhang mit bestimmten Anwendungen, dass alle elektrischen Geräte, die zum Schutz der Arbeitnehmer eingesetzt werden, von einem von OSHA genehmigten Nationally Recognized Testing Laboratory (NRTL) für die vorgesehene Anwendung genehmigt werden
(siehe z.B.: www.osha.gov/ ...Standard Interpretations ... 08/11/1994 - Presence sensing devices (PSDs) for power presses.: "...OSHA requires that all electrical products used by employees must be treated and approved for their intended use by an OSHA Approved Nationally Recognized Testing Laboratory (NRTL)....").

Anwendung weiterer Standards

Neben den OSHA Regeln, ist es wichtig die aktuellen Standards von Organisationen wie NFPA und ANSI sowie die in USA bestehende umfassende Produkthaftung zu beachten. Durch die Produkthaftung werden Hersteller und Betreiber im eigenen Interesse zur sorgfältigen Einhaltung von Vorschriften und zur Erfüllung des Standes der Technik "gezwungen".

Haftpflichtversicherungen verlangen im allgemeinen, dass ihre Versicherungsnehmer die anwendbaren Standards der Standardisierungsorganisationen erfüllen. Selbstversicherte Unternehmen haben diese Anforderung zunächst nicht, müssen aber im Falle eines Unfalles nachweisen, dass sie die allgemein anerkannten Sicherheitsprinzipien angewendet haben.

Zwei besonders wichtige Standards für Sicherheit in der Industrie sind NPFA 70 (bekannt als National Electric Code (NEC)) und NFPA 79 (Electrical Standard for industrial Machinery). Beide beschreiben die grundlegenden Anforderungen an die Eigenschaften und die Ausführung der elektrischen Ausrüstung. Der National Electric Code (NFPA 70) gilt vorrangig für Gebäude aber auch für die elektrischen Verbindungen von Maschinen und Teilmaschinen. NFPA 79 gilt für Maschinen. Damit besteht ein Graubereich in der Abgrenzung zwischen beiden Standards bei großen Maschinen, die aus Teilmaschinen bestehen. Z.B. große Fördersysteme können als Teil des Gebäudes betrachtet werden, so dass NFPA 70 und/oder NFPA 79 anzuwenden sind.

NFPA 79

Dieser Standard gilt für die elektrische Ausrüstung von Industriemaschinen mit Nennspannungen kleiner 600 V. (Als eine Maschine wird auch eine Gruppe von Maschinen, die koordiniert zusammenarbeiten, betrachtet.)
Die Neufassung NFPA 79 - 2002 enthält grundlegende Anforderungen für programmierbare Elektronik und Feldbusse, wenn diese zur Ausführung sicherheitsrelevanter Funktionen eingesetzt werden. Bei Erfüllung dieser Anforderungen dürfen besonders qualifizierte elektronische Steuerungen und Feldbusse auch für Not-Halt Funktionen der Stop Kategorien 0 und 1 verwendet werden (siehe NFPA 79 - 2002 9.2.5.4.1.4). Im Unterschied zu EN 60204-1 verlangt NFPA 79 bei Not-Halt Funktionen die elektrische Energie durch elektromechanische Mittel abzutrennen.

Die Kernanforderungen an programmierbare Elektronik und Busse sind: Systemanforderungen
(siehe NFPA 79 - 2002 9.4.3)

- Steuerungssysteme, die Software basierte Controller enthalten müssen,
  (1) falls ein einzelner Fehler auftritt,
    - zum Abschalten des Systems in einen sicheren Zustand führen
    - Wiederanlauf verhindern bis der Fehler beseitigt ist
    - unerwarteten Anlauf verhindern
  (2) vergleichbaren Schutz wie festverdrahtete Steuerungen bieten
  (3) entsprechend einem anerkannten Standard, der Anforderungen für solche Systeme definiert, ausgeführt sein.
  Als geeigneter Standard wird IEC 61508 in einer Note genannt.

Anforderungen an programmierbare Betriebsmittel (siehe NFPA 79 - 2002 11.3.4)

- Software und Firmware basierte Controller, die in sicherheitsrelevanten Funktionen eingesetzt werden, müssen für solche Anwendung gelistet sein (d.h. durch ein NRTL zertifiziert sein).
  In einer Note wird gesagt, dass IEC 61508 Anforderungen zum Design solcher Controller liefert.

Listing-Dateien elektronischer Geräte für Sicherheitsfunktionen

Zur Umsetzung der Anforderung in der NFPA 79: 2002 hat UL eine spezielle Kategorie für „Programmable Safety Controllers" (Bezeichnungscode NRGF) definiert. Diese Kategorie behandelt Steuerungsgeräte, die Software beinhalten und zur Anwendung in Sicherheitsfunktionen vorgesehen sind.

Die genaue Beschreibung der Kategorie sowie die Liste der Geräte, die diese Anforderung erfüllen, sind im Internet zu finden:

www.ul.com –> certifications directory –> UL Category code / Guide information –> search for category "NRGF"

TUV Rheinland of North America, Inc. ist ebenfalls NRTL für diese Anwendungen. Die dort gelisteten Produkte können auch im Internet angezeigt werden: Von der Home Page (http://www.tuv.com) aus kann mit der „ID" des Gerätes (Enter TUVdotCOM ID) die im Listing eingetragene Beschreibung abgerufen werden.

URL: http://www.tuv.com

ANSI B11

Die ANSI B11-Normen sind gemeinsame Standards/Normen, die von Gremien wie z.B. der Association for Manufacturing Technology (AMT – Vereinigung für Fertigungstechnologien), National Fire Protection Association (NFPA – Staatlicher Brandschutzverband) und der Robotic Industries Association (RIA - Roboterindustrieverband) entwickelt wurden.

Mit Hilfe der Risikoanalyse werden die Gefahren einer Maschine bewertet. Risikoanalyse ist eine wichtige Anforderung gemäß NFPA79-2002, ANSI/RIA 15.06 1999, ANSI B11.TR-3 und SEMI S10 (Halbleiter). Mit Hilfe der dokumentierten Ergebnisse einer Risikoanalyse kann die geeignete Sicherheitstechnik ausgewählt werden, basierend auf der gegebenen Sicherheitsklasse der jeweiligen Anwendung.

Die aktuellen Listen der ANSI-Normen finden Sie nachstehend. Sie dienen als Referenz, und falls eine genehmigte Überarbeitung diese ablösen sollten, so gilt die überarbeitete Norm.

Allgemeine Gesichtspunkte

ANSI B11.TR-1 (1993)
Ergonomic Guidelines for the design. installation and use of machine tools

ANSI B11.TR-2 (1997)
Mist control considerations for the design, installation and use of machine tools using metalworking fluids

ANSI B11.TR-3 (2000)
Risk assessment and risk reduction – A guide to estimate, evaluate and reduce risks associated with machine tools

ANSI B11.TR-4
Application of programmable electronic systems for the safety related functions of machines covered by the B11 safety standard series

ANSI Z244.1 (2003)
Control of hazardous energy- Lockout/tagout and alternative methods

ANSI Z535.1 (2002)
Safety Color Code

ANSI Z535.3 (2002)
Criteria for Safety Symbols

ANSI Z535.4 (2002)
Product Safety Signs and Labels

ANSI Z535.5 (2002)
Accident Prevention Tags and Labels

Weitere Referenznormen mit speziellen Festlegungen und weiteren Informationen:

OSHA 29CFR 1910.147
Control of hazardous energy ("lockout/tagout")

IEC 61496 (2003)
Safety of machinery; Electrosensitive protective equipment

Normen für den jeweiligen Maschinentyp

ANSI B11.1 (2001)
Safety requirements for Mechanical Power Presses

ANSI B11.2 (1995)
Safety requirements for Hydraulic Power Presses

ANSI B11.3 (2002)
Safety requirements for Power Press Brakes

ANSI B11.4 (2003)
Safety requirements for Shears

ANSI B11.5 (2002)
Iron Workers - Safety requirements for construction, care and use

ANSI B11.6 (2001)
Safety Requirements for Manual Tuning Machines

ANSI B11.7 (2000)
Cold Headers and Cold Formers - Safety requirements for construction, care and use

ANSI B11.8 (2001)
Safety requirements for Manual milling and boring Machines

ANSI B11.9 (1997)
Grinding machines - Safety Requirements for Construction Care and Use

ANSI B11.10 (2003)
Metal Sawing Machines - Safety Requirements for Construction Care and Use

ANSI B 11.11 (2001)
Safety Requirements for Gear & Spline Cutting Machines

ANSI B11.12 (1996)
Roll Forming and Roll Bending machines – Safety Requirements for Construction Care and Use

ANSI B11.13 (1998)
Automatic Screw/Bar and Chucking machines- Safety Requirements for Construction Care and Use

ANSI B11.14 (1996)
Coil Slitting Machines - Safety Requirements for Construction Care and Use

ANSI B11.15 (2001)
Safety Requirements for Pipe. Tube and Shape Bending Machines

ANSI B11.17 (1996)
Horizontal Hydraulic Extrusion Presses - Safety Requirements for Construction Care and Use

ANSI B11.18 (1997)
Coil Processing Systems - Safety Requirements for Construction Care and Use

ANSI B11.19 (2003)
Performance Criteria for Safeguarding

ANSI B11.20 (1996)
Manufacturing systems / Cells - Safety Requirements for Construction Care and Use

ANSI B11.21 (1997)
MachineTools Using Lasers - Safety Requirements for Construction Care and Use

ANSI B11.22 (2002)
Safety Requirements for Numerical Controlled Turning Machines

ANSI B11.23 (2002)
Safety Requirements la Machine Centers

ANSI B11.24 (2002)
Safety Requirements for Transfer Machines

Prozessindustrie in USA

Die grundlegenden Sicherheitsanforderungen der OSHA für die Prozessindustrie sind in OSHA´s Process Safety Management of Highly Hazardous Chemicals, Explosives and Blasting Agents Standard (PSM), 29 CFR 1910.119 beschrieben. (Siehe www.osha.gov).

Zitate aus 29 CFR 1910.119:

Purpose. This section contains requirements for preventing or minimizing the consequences of catastrophic releases of toxic, reactive, flammable, or explosive chemicals. These releases may result in toxic, fire or explosion hazards.
Abschnitt (d) mit seinen Unterabschnitten enthält die Grundanforderungen an die Prozeßinstrumentierung.

1910.119(d)
Process safety information. ... the employer shall complete a compilation of written process safety information ... This process safety information shall include information pertaining to the hazards of the highly hazardous chemicals used or produced by the process, information pertaining to the technology of the process, and information pertaining to the equipment in the process.

1910.119(d)(3)
Information pertaining to the equipment in the process.

1910.119(d)(3)(i)(F)
Design codes and standards employed;

1910.119(d)(3)(ii)
The employer shall document that equipment complies with recognized and generally accepted good engineering practices.

Guidelines dazu gibt OSHA mit: CPL 2-2.45A "Process Safety Management of Highly Hazardous Chemicals-- Compliance Guidelines and Enforcement Procedures.

OSHA verlangt, dass die Prozessinstrumentierung gemäß anerkannter und allgemein akzeptierter "good engineering practice" ausgeführt wird. Mit Schreiben vom März 2000 stellt OSHA auf eine entsprechende Anfrage von ISA klar, dass ANSI/ISA 84.01 ein Standard mit nationaler Übereinstimmung ist und von OSHA als allgemein akzeptierte "good engineering practice" anerkannt wird. Mit dem selben Schreiben stellt OSHA aber auch klar, dass ISA 84.01 nicht grundsätzlich als der einzige Standard zum erfüllen der Anforderungen von 1910.119 (PSM) betrachtet wird.

Aus CFR 1910.119 geht zunächst nicht klar hervor, ob die Anforderungen sich auf die vollständige Instrumentierung beziehen. In der Prozessindustrie sind zwei Typen der Instrumentierung üblich. "Safety Instrumented Systems" (SIS) und "Basic Process Control System" (BPCS). ANSI/ISA 91.01 definiert, dass nur das SIS unter den OSHA Regeln zu behandeln ist.

IEC 61511 "Functional safety: Safety Instrumented Systems for the process industry sector" ist der IEC Standard mit dem gleichen Scope wie ISA 84.01. Er wurde unter starker Beteiligung von ISA entwickelt und soll als Neufassung der ISA 84 übernommen werden.

Ein großer Teil von Prozessen ist im Scope von ISA 84.01, fällt aber formal nicht unter 29 CFR 1910.119 (PSM). Auch hier sollte der Standard angewendet werden, um nicht die grundsätzlichen Anforderungen des "Duties" Abschnittes des Occupational Safety and Health Act (OSHA) zu verletzen.

Arbeitsschutzbestimmungen und Sicherheitsnormen in Kanada

Das Kanadische Arbeitsgesetzbuch (Canada Labour Code) ist das für alle Industriezweige Kanadas gültige Gesetz. Teil 2 des Kanadischen Arbeitsgesetzbuches befasst sich mit der Sicherheit und dem Gesundheitsschutz am Arbeitsplatz. Nach der kanadischen Verfassung sind in erster Linie die Provinzbehörden für das Arbeitsrecht zuständig. Im Arbeitsschutzgesetz (Occupational Health and Safety Act, OHSA) werden die Rechte und Pflichten aller betrieblichen Parteien festgelegt. Sein Hauptzweck ist der Schutz der Arbeitnehmer vor Gesundheits- und Sicherheitsrisiken bei der Arbeit. Das OHSA setzt Verfahren für den Umgang mit Risiken am Arbeitsplatz fest. Wird das Gesetz nicht freiwillig erfüllt, sieht es dessen Vollstreckung vor. Die kraft dem OHSA erlassenen Verordnungen beinhalten bestimmte Anforderungen, Normen und Verfahrensweisen, die zur Verringerung der Gefahr von Arbeitsunfällen einzuhalten sind.

Von der Bundes- bzw. den Provinz- oder Gebietsregierungen bestellte Beamte sind dazu befugt, Arbeitsplätze zu besichtigen. Darüber hinaus können sie den Vollzug des Gesetzes durch sämtliche erforderliche Vollzugsmittel erwirken, die sich an Arbeitgeber und Arbeitsnehmer richten. Hierzu gehören auch Anordnungen zur Arbeitseinstellung, Geldstrafen und eine strafrechtliche Verfolgung. Hierzu gehören beispielsweise das Arbeitsministerium (MoL) in Ontario oder die Kommission für Gesundheit und Sicherheit bei der Arbeit (CSST) in Quebec. Die Beamten arbeiten eng mit ihren Geschäftsstellen, Verbänden für Sicherheit am Arbeitsplatz (Safe workplace associations, SWAs), Schulungszentren und Kliniken für Arbeitnehmer sowie dem Kanadischen Zentrum für Sicherheit und Gesundheitsschutz am Arbeitsplatz zusammen. Zu diesen leitenden Organisationen gehören auch der Verband zur Unfallverhütung an industriellen Arbeitsplätzen (Industrial Accident Prevention Association, IAPA) in Ontario und das Institut de Reherche Robert-Sauvé en Santé et en Sécurité du Travail (IRSST) in Quebec. Versicherungskammern spielen ebenfalls eine wichtige Rolle bei der Sicherheit am Arbeitsplatz. Beispielsweise beaufsichtigt die Versicherungskammer für Sicherheit am Arbeitsplatz (Workplace Safety and Insurance Board, WSIB) das Ausbildungs- und Schulungssystem für Sicherheit am Arbeitsplatz, zahlt Berufsunfähigkeitsrenten im Rahmen des Unfallversicherungsprogramms aus, überwacht die Qualität der Gesundheitsvorsorge durch den Einsatz finanzieller Maßnahmen usw.

Regierung von Kanada, Sicherheit und Gesundheitsschutz am Arbeitsplatz in Kanada (www.hrsdc.gc.ca)

Arbeitsministerium (www.gov.on.ca/lab/)

Commission de la santé et de la sécurité du travail (www.csst.qc.ca)

Verband zur Unfallverhütung an industriellen Arbeitsplätzen (www.iapa.on.ca)

Das Institut de Recherche Robert-Sauvé en Santé et en Sécurité du Travail (www.irsst.qc.ca)

Sicherheit am Arbeitsplatz & Versicherungskammer (www.wsib.on.ca)

Die Verordnung für Industrieunternehmen nach dem OHSA in Ontario, Verordnung 528/00 Abschnitt 7 (PSHSR - Pre Start Health and Safety Review, Pre-Start-Sicherheits- und Gesundheitsprüfungen) ist seit dem 7. Oktober 2000 in Kraft, wobei sich der 2. Punkt der Tabelle auf die Sicherheit von Maschinen bezieht. Der Arbeitgeber hat sicherzustellen, dass der Arbeitsplatz sämtlichen Anforderungen des OHSA sowie den Verordnungen Genüge leistet. Die Verordnung ist größtenteils eine leistungsbasierte Norm, d.h., sie bestimmt die anzuwendende Sicherheitsebene sowie das beabsichtigte Ziel, legt jedoch nicht fest wie die geforderte Sicherheitsebene zu erreichen ist.

Abschnitt 7 oder Verordnung 528/00 bezieht sich auf die gegenwärtig in Kanada geltenden Normen. Um die Anforderungen aus Abschnitt 7 vollständig zu erfüllen, muss Bezug auf andere anerkannte geltende Richtlinien und Normen genommen werden, beispielsweise die Brandschutzrichtlinien von Ontario (Ontario Fire Code), die Nationalen Brandschutzrichtlinien (National Fire code), die NFPA-Gesetze und -Normen, CSA-Gesetze und -Normen, ANSI-Normen usw. Die dargestellte Tabelle ist eine Zusammenfassung der für die Maschinensicherheitsumstände geltenden Normen. Diese werden als Hilfestellung zur Erfüllung von Abschnitt 7 der Verordnung aufgelistet.

“Richtlinien für Pre-Start-Sicherheits- und Gesundheitsprüfungen (Pre-Start Health and Safety Reviews)”, April 2001, Arbeitsministerium

Geltende Bestimmungen der Verordnung	Umstände	Ontario Richtlinien	Grundnormen (‘A’ & ‘B’)	Maschinenspezifisch Normen ‘C’
Abschn. 24, 25, 26, 28, 31 und 32	Gilt, wenn eine der folgenden Vorrichtungen als Schutzelement in Verbindung mit einem Gerät verwendet wird: 1. Sicherheitsvorrichtungen, die dem Gerät ein Signal zum Anhalten übermitteln, einschließlich unter anderem Lichtvorhänge und Sicherheitsglasscheiben, Überwachungssysteme mit Abtastbereich, Funksysteme, Zweihand-Steuerungssysteme, Systeme mit Zweihandauslösung sowie Ein- oder Mehrstrahlsysteme 2. Schutzgitter mit verriegelnden mechanischen oder elektrischen Sicherheitsvorrichtungen	Ontario Elektrische Sicherheitsrichtlinien	CSA-Z432* ANSI B11.19 ISO 14121 ISO 12100 Parts 1&2 ISO 13851 ISO 13852 ISO 13853 ISO 13854 ISO 13855 ISO 13856 ISO 14119 ISO 14120 IEC 61496 Parts 1,2,3 ISO 4413 ISO 4414	CSA Z142* CSA Z434* CSA Z615i ANSI B11.1* ANSI B11.2 ANSI B11.3 ANSI B11.6 ANSI B11.8 ANSI B11.10 ANSI B11.20 ANSI B11.21 ANSI B65.1 ANSI B65.2 ANSI B65.5 ANSI 15.06 ANSI B151.1 ANSI Z245.1 +MOL Guide ANSI Z245.2 ANSI Z245.5

* Letzte Änderung gilt

Bei A-&-B-Normen handelt es sich um Sicherheitsgrundnormen, die grundlegende Konzepte und Richtlinien für Konstruktions- und allgemeine Aspekte vorgeben beziehungsweise sich auf einen Sicherheitsaspekt oder eine Art sicherheitsbezogener Vorrichtung beziehen, die auf Maschinen oder Prozesse angewandt werden kann.

Bei C-Normen handelt es sich um Sicherheitsstandards, die sich auf detaillierte Sicherheitsanforderungen für eine bestimmte Maschine oder einen bestimmten Prozess beziehen.

Folgendes sind die **wichtigsten Normwerke für Maschinensicherheit in Kanada**, die die Verwendung sicherheitsbezogener soft- und firmwarebasierter Steuerungen einschließlich deren neuester Änderungen anerkennen:

- CSA Z432-04 „Maschinensicherheit" erkennt die Verwendung einer programmierbaren Sicherheitssteuerung nach Abschnitt 8.3 an.
  Diese Norm bezieht sich auf den Schutz von Personen vor Risiken, die aus der Verwendung mobiler oder ortsfester Maschinen herrühren. Sie gibt die einzuhaltenden Kriterien sowie die Beschreibung, Auswahl und Anwendung von Schutz- und Sicherheitsvorrichtungen vor. Ist eine gegenwärtige CSA-Norm für eine bestimmte Maschinenart vorhanden, muss diese gemeinsam mit dieser Norm angewandt werden, um den bestmöglichen Schutz für diese besondere Situation zu erzielen.

- CSA Z434-03 „Industrieroboter und allgemeine Sicherheitsanforderungen für Robotersysteme" erkennt die Verwendung einer programmierbaren Sicherheitssteuerung nach Abschnitt 6.5 an.
  Ziel dieser Norm ist die Vorgabe von Anforderungen für die Fertigung mit Industrierobotern, die Wiederaufarbeitung und den Neuaufbau

sowie die Integration/Installation von Robotersystemen, weiterhin die Vorgabe von Schutzmethoden zur Verbesserung der Sicherheit des Personals, das der Verwendung von Robotern und Robotersystemen zugeordnet ist.

- CSA Z142-02 „Richtlinie für den Betrieb mechanischer Pressen: Gesundheit, Sicherheit und Schutzmaßnahmen" erkennt die Verwendung einer programmierbaren Sicherheitssteuerung nach Abschnitt 8.1.3 an.
  Diese Norm widmet sich den Anforderungen des Arbeitsschutzes und der Sicherheit für mechanische Pressen aller Art, die mit Stößel (Plungerkolben oder Schlitten) und Druckplatten für das Stanzen, Schneiden, Beschneiden, Ziehen, Lochen, Umformen (Biegen), Prägen oder die Verarbeitung von Metall oder anderen Materialien ausgestattet sind.

- NFPA 79 2002 „Elektrische Norm für Industriemaschinen" erkennt die Verwendung einer programmierbaren Sicherheitssteuerung nach Abschnitt 9.4.3. und Abschnitt 11.3.4. an.
  Diese Norm gibt detaillierte Informationen für die Anwendung elektrischer/elektronischer Einrichtungen, Geräte oder Systeme, die als Teil von Industriemaschinen geliefert werden und Sicherheit für Personen und Sacheigentum bieten. Die Bestimmungen dieser Norm gelten für elektrische/elektronische Einrichtungen, Geräte oder Systeme von Industriemaschinen, die mit einer Nennspannung von maximal 600 Volt arbeiten, beginnend am Anschlusspunkt der Energieversorgung für die elektrische Einrichtung der Maschine.

Die CSA-Sicherheitsnormen erfordern die Zertifizierung der sicherheitsbezogenen soft- und firmwarebasierten Sicherheitssteuerungen durch ein landesweit anerkanntes Prüflabor (Nationally Recognized Testing Laboratory, NRTL) oder ein vom Normungsausschuss von Kanada (Standards Council of Canada, SCC) zugelassenes Prüflabor gemäß einem für Sicherheitsvorrichtung anerkannten geltenden Standard.

Sorgfaltspflichtverletzung in Sicherheitsfragen ist eine strafbare Handlung

- Die Gesetzesvorlage C-45 ist ein neues Gesetz des Strafgesetzbuchs, rechtswirksam ab 31. März 2004.

- Das Kanadische Arbeitsgesetzbuch erlegt Arbeitgebern und Personen, die produktive Arbeiten ausführen, eine Rechtspflicht kraft Strafgesetzbuch auf, angemessene Maßnahmen zum Schutz von Arbeitnehmern und zur öffentlichen Sicherheit zu ergreifen.

- Eine Organisation kann von jetzt an der strafbaren Fahrlässigkeit in Gesundheits- und Sicherheitsfragen angeklagt werden, weshalb gegen selbige kraft Arbeitsschutzgesetztes und Strafgesetzbuch ein Ermittlungsverfahren und eine Anklage eröffnet werden kann.

- Kraft der Gesetzesvorlage C-45 wird die maximale Geldstrafe bei einer Verurteilung wegen Ordnungswidrigkeit von $25.000 auf $100.000 erhöht. Für schwerere Vergehen ist der Geldstrafe nach oben keine Grenze gesetzt.

- Die Höchststrafe bei einer Verurteilung wegen strafbarer Fahrlässigkeit ist eine lebenslange Freiheitsstrafe.

Regierung von Kanada, Sicherheit und Gesundheitsschutz am Arbeitsplatz in Kanada (www.hrsdc.gc.ca)

Hoheitsakte zur besseren Vollstreckbarkeit von Arbeitsschutzgesetzen

Die Regierung Kanadas kündigte am 8. Juli 2004 200 zusätzliche Arbeitsschutzinspektoren an, deren Ziel Arbeitsplätze mit mangelndem Arbeitsschutz sein werden. Ziel der Regierung ist es, Verletzungen am Arbeitsplatz in vier Jahren um 20% zu senken. Ausgehend von den Durchschnittskosten für eine Verletzung am Arbeitsplatz, würde sich eine Vermeidung von 60.000 Verletzungen pro Jahr in Form einer Ersparnis von jährlich $960 Millionen auswirken. Die Anstellung von 100 neuen Inspektoren setzte unmittelbar ein, wodurch die Zahl der gegenwärtig tätigen 230 Inspektoren erheblich aufgestockt wird. Anfängliches Ziel der Inspektoren werden 6.000 Arbeitsplätze mit den höchsten Verletzungsraten sein.

04-78, July 8, 2004, Ministry of Labour (www.gov.on.ca/lab/)

1.4 Sicherheitsanforderungen für Maschinen in Japan

Zur Anwendung im Inland

Die Situation in Japan war bisher anders als in Europa und USA. Im Gegensatz zu Europa und USA, wo der Arbeitgeber für die Sicherheit am Arbeitsplatz verantwortlich ist, muss in Japan der Arbeitnehmer selber darauf achten, dass ihm nichts passiert. Er darf deshalb nur entsprechend geschultes Personal an eine Maschine.

Vergleichbare gesetzliche Anforderungen zur funktionalen Sicherheit wie in Europa existierten folglich nicht. Ebenso spielt die Produkthaftung keine solche Rolle wie in USA. Inzwischen hat man aber erkannt, dass dieses Konzept heute nicht mehr reicht. Man geht zu dem Grundprinzip wie in Europa und USA über.

Es gibt keine gesetzliche Anforderung zur Anwendung von Normen, aber eine Verwaltungsempfehlung zur Anwendung von JISs (Japanese Industrial Standards):
Japan lehnt sich an das europäische Konzept an und hat grundlegenden Normen als nationale Standards übernommen (siehe Tabelle)

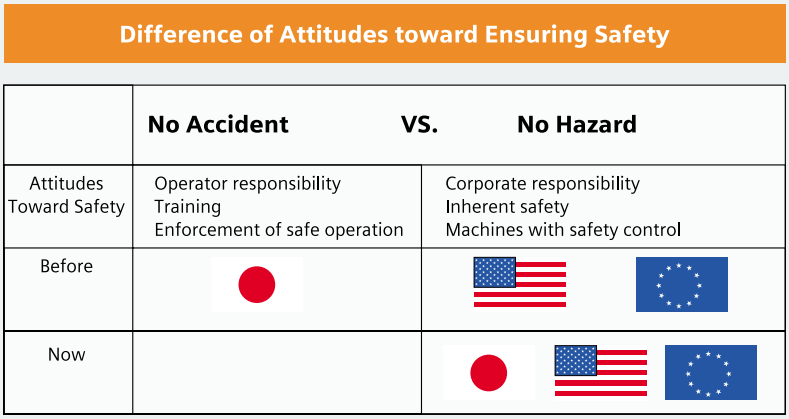


Bild 1/15
Wandel des Verantwortungskonzeptes für Maschinensicherheit in Japan (aus: Toshihiro Fujita et.al.: „NECA Activities for Meeting Globalized Standards and Certification", Robot, Japan Robot Association, March 2004)

ISO/IEC number	JIS number	Note
ISO12100-1	JIS B 9700-1	frühere Bezeichnung TR B 0008
ISO12100-2	JIS B 9700-2	frühere Bezeichnung TR B 0009
ISO14121 (EN1050)	JIS B 9702	
ISO13849-1 (Ed. 1)	JIS B 9705-1	
ISO13849-2 (Ed. 2)	JIS B 9705-1	
IEC60204-1	JIS B 9960-1	ohne Annex F bzw. Route Map des europäischen Vorwortes
IEC1508-1 to 7	JIS C 0508	
IEC 62061		noch keine JIS Nummer vergeben

Für global operierende Maschinenhersteller und -anwender

Exportorientierte japanische Maschinenhersteller haben ein dringendes Interesse, die europäischen und amerikanischen Anforderungen zu erfüllen, damit ihre Produkte den Anforderungen der Zielmärkte genügen. Firmen mit global verteilten Fertigungsstätten orientieren sich ebenfalls an den europäischen und amerikanischen Anforderungen, um möglichst einheitliche Sicherheitskonzepte in allen Fabriken zu haben.

1.5 Wichtige Adressen

Europa

1. CEN-Mitglieder = Bezugsquellen für nationale Fassungen von EN + prEN

AENOR
Asociación Española de Normalización
y Certificación (AENOR)
Génova, 6
E-28004 Madrid

Telefon: + 34 91 432 60 00
Telefax: + 34 91 310 31 72
E-mail: dzc@aenor.es

AFNOR

Association Française de Normalisation
11, Avenue Francis de PressenséF-
93571 Saint-Denis La Plaine Cedex

Telefon: + 33 1 41 62 80 00
Telefax: + 33 1 49 17 90 00

BSI

British Standards Institution
389 Chiswick High Road
GB-London W4 4AL

Telefon: + 44 208 996 90 00
Telefax: + 44 208 996 74 00

E-mail: first name_surname@bsi-global.com
E-mail: info@bsi-global.com

COSMIT

Czech Standards Institute
Biskupsky dvùr 5
CZ-110 02 Praha 1

Telefon: +420 2 218 02 111
Telefax: +420 2 218 02 301
E-mail : info@csni.cz

DIN

Deutsches Institut für Normung e.V.
Burggrafenstr. 6
D-10787 Berlin

Telefon: + 49 30 26 01 0
Telefax: + 49 30 26 01 12 31
E-mail: postmaster@din.de

DS

Dansk Standard
Kollegievej 6
DK-2920 Charlottenlund

Telefon: + 45 39 96 61 01
Telefax: + 45 39 96 61 02
E-mail: dansk.standard@ds.dk

ELOT

Hellenic Organization
for Standardization
313, Acharnon Street
GR-11145 Athens

Telefon: + 30 1 212 01 00
TX: (0601) 219670 elot gr
Telefax: + 30 1 228 62 19
E-mail: info@elot.gr

IBN/BIN

Institut Belge de Normalisation/
Belgisch Instituut voor Normalisatie
Avenue de la Brabançonne 29/
Brabançonnelaan 29
B-1000 Bruxelles/Brussel

Telefon: + 32 2 738 01 11
Telefax: + 32 2 733 42 64
E-mail: info@ibn.be

IPQ

Instituto Português da Qualidade
Rua António Gião, 2
P-2829-513 Caparica

Telefon: + 351 21 294 81 00
Telefax: + 351 21 294 81 01
E-mail: ipq@mail.ipq.pt

NEN

Nederlands Normalisatie-Instituut
Kalfjeslaan
Postbus 5059
NL-2600 GB Delft

Telefon: + 3115690390
Telefax: + 3115690190
E-mail: info@nen.nl

NSAI

National Standards Authority of Ireland
Glasnevin
IRL-Dublin 9

Telefon: + 353 1 807 38 00
Telefax: + 353 1 807 38 38
E-mail: nsai@nsai.ie

NSF

Norges Standardiseringsforbund
PO Box 353 Skøyen
N-0213 Oslo

Telefon: + 47 22 04 92 00
Telefax: + 47 22 04 92 11
E-mail: info@standard.no

ON

Österreichisches Normungsinstitut
Postfach 130
Heinestraße 38
A-1020 Wien

Telefon: + 43 1 213 00
Telefax: + 43 1 213 00 818
E-mail : office@on-norm.at

SEE

Service de L'Energie de l'Etat
Organisme Luxembourgeois
de Normalisation
B.P. 10
L-2010 Luxembourg

Telefon: + 352 46 97 46 1
Telefax:+ 352 22 25 24
E-mail: see.normalisation@eg.etat.lu

SFS

Suomen Standardisoimisliitto r.y.
PO Box 116
FIN-00240 Helsinki
Finland

Telefon: + 358 9 149 93 31
Telefax: + 358 9 146 49 25
E-mail: sfs@sfs.fi

SIS

Standardiseringen i Sverige
Box 6455
S-113 81 Stockholm

Telefon: + 46 8 610 30 00
Telefax: + 46 8 30 77 57
E-mail: info@sis.se

SNV

Schweizerische Normen-Vereinigung
Bürglistraße 29
CH-8400 Winterthur

Telefon: + 41 52 224 54 54
TX: (045) 755931 snv ch
Telefax: + 41 52 224 54 74
E-mail: info@snv.ch

STRI

Icelandic Council for Standardization
Laugavegur 178
IS-105 Reykjavik

Telefon: + 354 520 71 50
Telefax: + 354 520 71 71
E-mail: stri@stri.is

UNI

Ente Nazionale Italiano di Unificazione
Via Battistotti Sassi, 11b
I-20133 Milano MI

Telefon: + 39 02 70 02 41
Telefax: + 39 02 70 10 61 06
E-mail: uni@uni.com

CEN

European Comittee for Standardization-
Rue de Stassrt 36
B-1050 Bruxelles

Telefon: + 3225500811
Telefax: + 3225500819
E-mail: infodesk@cenorm.be

CENELEC

European Comittee for
Electrotechnical Standardization
Rue de Stassrt 35
B-1050 Bruxelles

Telefon: + 3225196871
Telefax: + 3225196919
E-mail: info@cenelec.org

2. DIN – Deutsches Institut für Normung e.V., Federführende Normenausschüsse in Bezug auf Maschinen

NAM

Normenausschuss Maschinenbau
(NAM)im DIN
Lyoner Str. 8
Postfach 710864
60498 Frankfurt/M.

Telefon: 069/6603-1341
Telefax: 069/6603-1557

NWM

Normenausschuss Werkzeugmaschinen
Corneliusstraße 4
60325 Frankfurt

Telefon: 069/75608123
Telefax: 069/75608111

AGSA, FNErg, FNFW, FNL, NAL, NALS, NAS, Nasg, NI, NKT, NMP, Textilnorm

DIN Deutsches Institut für Normung e.V.
10772 Berlin

Telefon: 030/2601-0
Telefax: 030/2601-1260

FNCA, FNKä, FWS, Naa, NAD, NL, NÖG, NRK, NÜA

DIN Deutsches Institut für Normung e.V.
Zweigstelle Köln
Kamekestraße 8
50672 Köln

Telefon: 0221/5713-0
Telefax: 0221/5713-414

NA EBM

Normenausschuss Eisen-, Blech- und Metallwaren
Kaiserwerther Str. 137
40474 Düsseldorf

Telefon: 0211/4564274/276
Telefax: 0211/4564277

NA FuO

Normenausschuss Feinmechanik und Optik
Turnplatz 2
75172 Pforzheim

Telefon: 07231/918822
Telefax: 07231/918833

FAKAU

Normenausschuss Kautschuktechnik
Zeppelinstr. 69
Postfach 900360
60487 Frankfurt/M.

Telefon: 069/7936-0/117
Telefax: 069/7936165

DKE

Deutsche Kommission Elektrotechnik Elektronik
Informationstechnik im DIN und VDE
Stresemannallee 15
60596 Frankfurt/M.

Telefon: 069/6308-0
Telefax: 069/9632925
E-mail: dke@vde.com

3.Bezugsquellen für technische Regelwerke in Deutschland

Für EG-Richtlinien sowie Gesetze und Verordnungen

Bundesanzeiger-Verlags GmbH
Amsterdamer Straße 192
50667 Köln

Telefon: (0221) 97668-0
Telefax: (0221)

Für DIN-Normen und VDM-Einheitsblätter

Beuth Verlag GmbH
Burggrafenstraße 6
10787 Berlin

Telefon: (030) 2601-0
Telefax: (030) 2601-1260

Für VDE-Vorschriften sowie Normen der DKE und IEC

VDE-Verlag GmbH
Bismarckstraße 33
10625 Berlin

Telefon: (030) 348001-16
Telefax: (030) 3417093

Für Unfallverhütungsvorschriften und ZH-1-Schriften der Berufsgenossenschaften

Carl Heymanns Verlag KG
Luxemburger Straße 449
50939 Köln

Telefon: (0221) 94373-0
Telefax: (0221) 94373-901

Alles über Normen, Vorschriften, Richtlinien

Deutsches Informationszentrum für

Technische Regeln (DITR) im DIN
(Deutsches Institut für Normung)
Burggrafenstraße 6
10787 Berlin

Telefon: (030) 2601-0
Telefax: (030) 2628125

Amerika

Zusätzliche Informationen über Maschinensicherheit

ANSI
(American National Standards Institute)
http://www.ansi.org

OSHA
(Occupational Safety and Health Administration)
http://www.osha.gov

NFPA
(National Fire Protection Association)
http://www.nfpa.org

TUV
Rheinland of N.A. Inc.
http://www.us.tuv.com

UL
(Underwriter Laboratories)
http://www.ul.com

CSA
(Canadian Standards Association)
http://www.csa.ca

CCOHS
(Canadian Center for Occupational - Health and Safety)
http://www.ccohs.ca

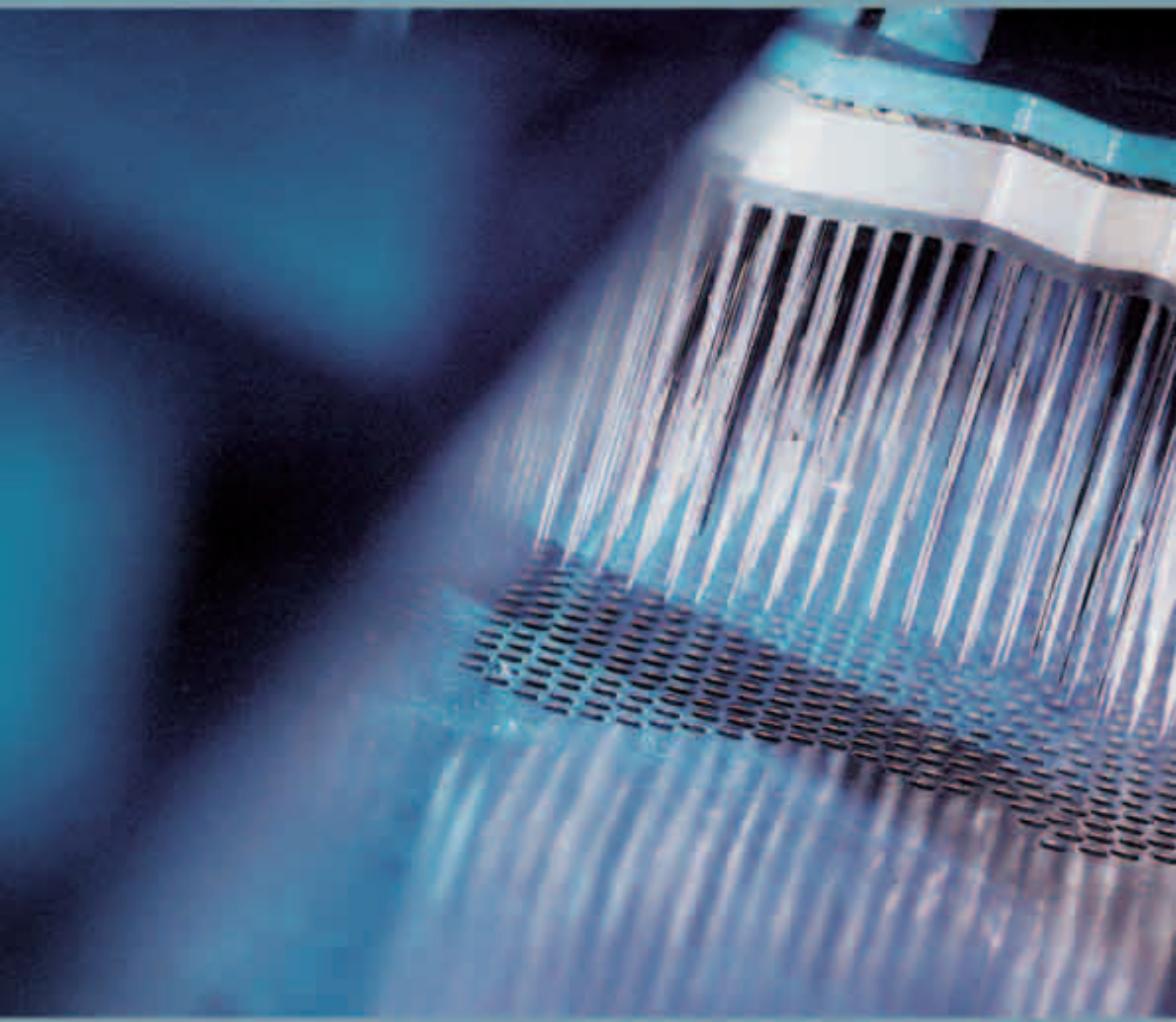
NIOSH
(National Institute of Occupational Health and Safety)
http://www.cdc.gov/niosh/homepage.html

NSC
(National Safety Council)
http://www.nsc.org

ASSE
(American Society of Safety Engineers)
http://www.asse.org

RIA
(Robotic Industries Association)
http://www.robotics.org

Global Engineering Documents
http://www.global.his.com



2.1 Überblick

2.2 Entwurfs- und Realisierungsprozess der Maschine, Risikobeurteilung, Prozess der Risikominderung

2.3 Hängt die Schutzmaßnahme von einer Steuerung ab?

2.4 Spezifikation der Sicherheitsanforderungen

2 Spezifikationen und Design sicherheitsrelevanter Steurungen für Maschinen

2.5 Entwurf und Realisierung der (sicherheitsrelevanten) Steuerung nach IEC 62061

2.6 Entwurf und Realisierung der sicherheitsbezogenen Teile einer Steuerung nach EN 954-1 (ISO 13849-1 (rev))

2 Spezifikation und Design sicherheitsrelevanter Steuerungen für Maschinen

2.1 Überblick

Die Struktur der folgenden Beschreibung basiert auf dem Lebenszyklusmodell, d.h. die Reihenfolge der einzelnen Abschnitte orientiert sich an der Reihenfolge, in der die einzelnen Phasen des Maschinen- und Anlagenengineerings normalerweise ausgeführt werden.

Sicherheit erfordert Schutz vor vielfältigen Gefährdungen. Im Folgenden wird die Funktionale Sicherheit behandelt. Das ist der Teil der Sicherheit einer Maschine oder Anlage, der von der korrekten Funktion ihrer Steuerungs- oder Schutzeinrichtungen abhängt. Fragen der Gefährdung durch andere Risiken wie z.B. Elektrizität, Wärme, Strahlung etc. werden ebenso wenig behandelt wie Aspekte der Wirtschaftlichkeit.

Die Beschreibung basiert auf den derzeit gültigen Sicherheitsanforderungen in Europa. Dabei werden aber zu erwartende Änderungen, soweit sie bereits bekannt sind, berücksichtigt. Ebenso wird ggf. auf abweichende Anforderungen für die Anwendung außerhalb Europas eingegangen.

Wegen der unterschiedlichen Vorschriften und Normen werden Maschinen und Prozessanlagen getrennt betrachtet, auch wenn die Grundprinzipien, mit denen die Sicherheit erreicht wird, gleich sind.

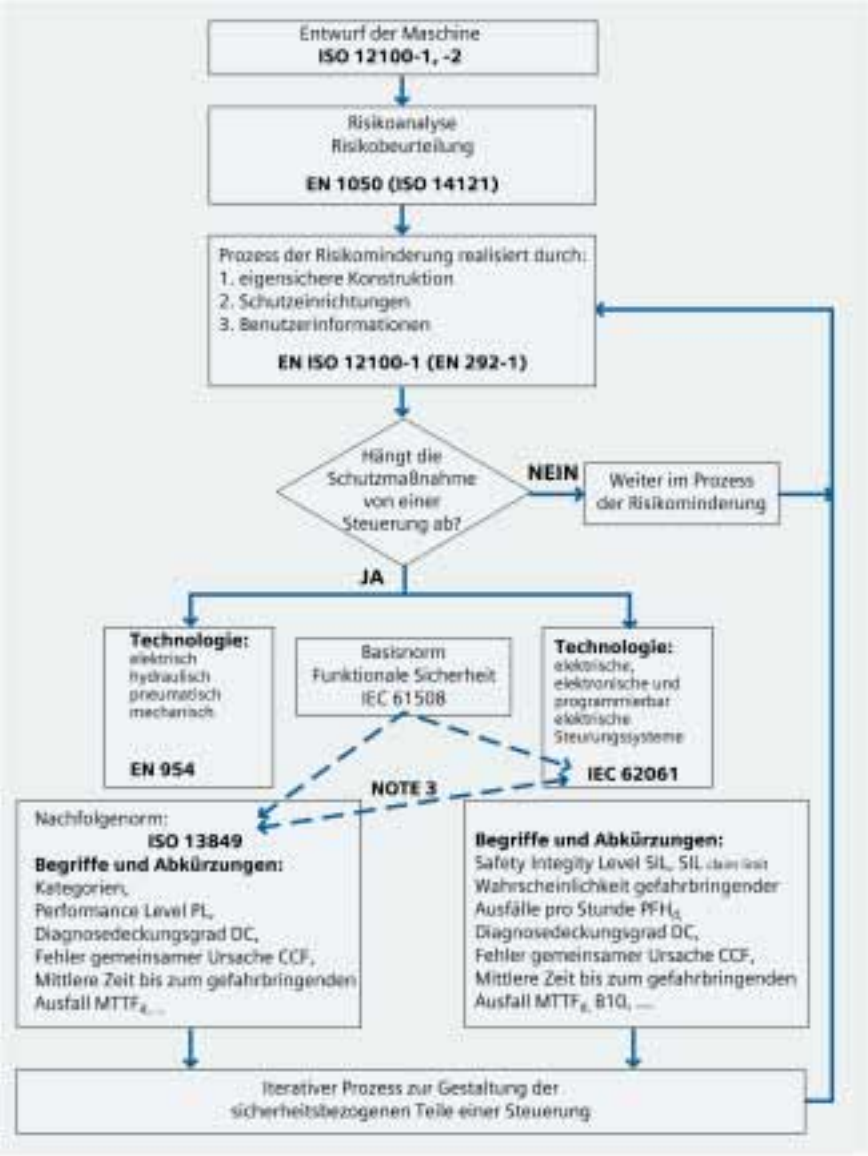


Bild 2/1
Designprozess einer Maschine Note 3: Für nicht elektrische Technologien: Verwenden Sie Teile die der EN ISO 13849-1 (rev) entsprechen, als Teilsysteme

[1] Der Begriff „Maschine" beinhaltet im folgenden auch Kombinationen von Maschinen, d.h. „integrierte Fertigungssysteme".

2.2 Entwurfs- und Realisierungsprozess der Maschine, Risikobeurteilung, Prozess der Risikominderung

Der Lebenszyklus einer Maschine gliedert sich grob in die in Bild 2/1 dargestellten Abschnitte. Die einzelnen Phasen umfassen jeweils klar abgrenzbare Aufgaben, so dass die Ausführung bestimmter Schritte durch unterschiedliche Personen oder Organisationen erfolgen kann.

Eine Strategie zur Risikoreduzierung einer Maschine ist in ISO 12100-1 Kap. 5 beschrieben. Dort wird auch klar gesagt, welche Priorität den verschiedenen Aspekten des Maschinendesigns einzuräumen ist.

Bei der Durchführung dieses Prozesses ist es erforderlich, folgende Rangfolge des Vorgehens zu berücksichtigen:

- Sicherheit der Maschine in sämtlichen Phasen ihrer Lebensdauer
- Fähigkeit einer Maschine, ihre Funktion auszuführen
- Benutzerfreundlichkeit der Maschine
- Herstellungs-, Betriebs- und Demontagekosten der Maschine

Die Risikoreduzierung einer Maschine erfolgt in einem iterativen Prozess. Die einzelnen Schritte dazu sind in EN 1050 beschrieben (siehe auch Kapitel 1 dieses Handbuches). Der Prozess der Risikoreduzierung umfasst die Risikobeurteilung und sofern notwendig die Bestimmung von Maßnahmen zur Risikoreduzierung.

In ISO 12100-2 sind grundlegende, technische Prinzipen beschrieben, die

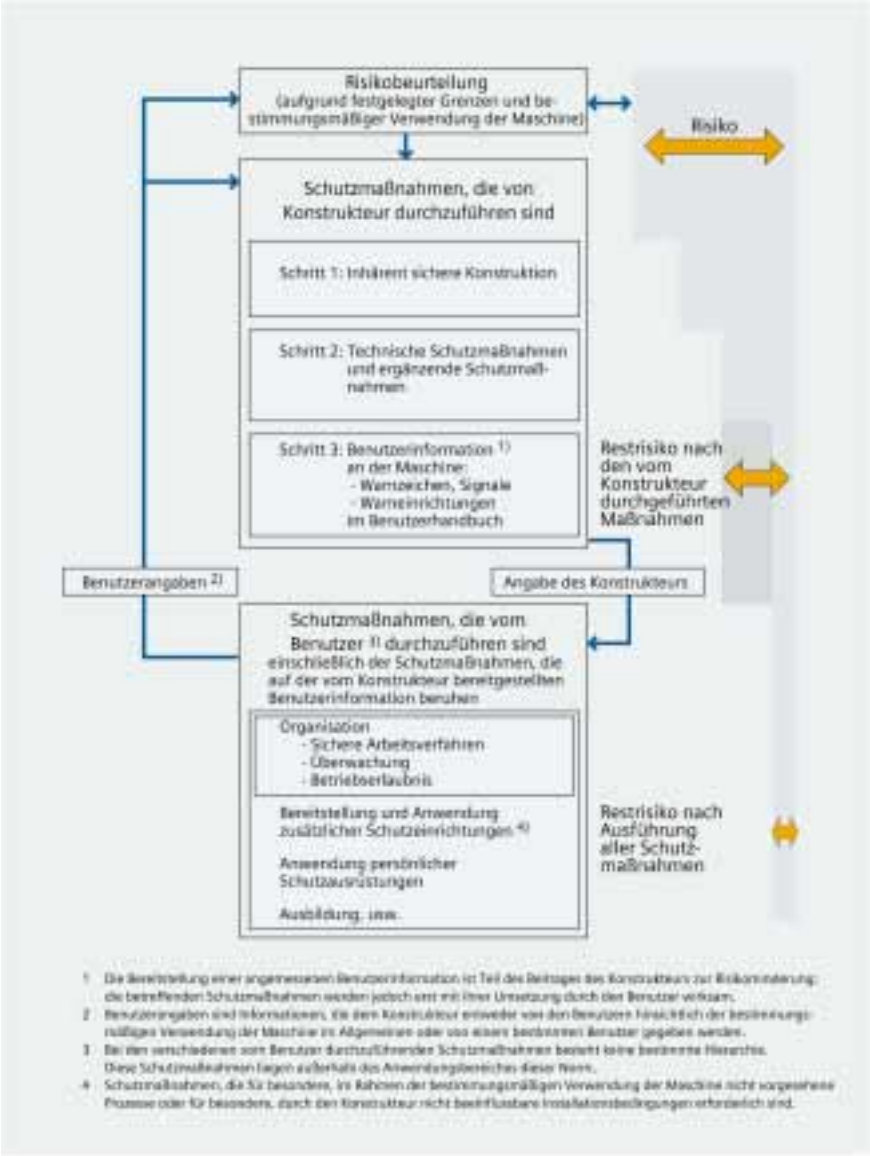

Risikobeurteilung
(aufgrund festgelegter Grenzen und bestimmungsmäßiger Verwendung der Maschine)
Risiko
Schutzmaßnahmen, die vom Konstrukteur durchzuführen sind
Schritt 1: Inhärent sichere Konstruktion
Schritt 2: Technische Schutzmaßnahmen und ergänzende Schutzmaßnahmen
Schritt 3: Benutzerinformation 1)
an der Maschine:
- Warnzeichen, Signale
- Warneinrichtungen
im Benutzerhandbuch
Restrisiko nach den vom Konstrukteur durchgeführten Maßnahmen
Benutzerangaben 2)
Angabe des Konstrukteurs
Schutzmaßnahmen, die vom Benutzer 3) durchzuführen sind einschließlich der Schutzmaßnahmen, die auf der vom Konstrukteur bereitgestellten Benutzerinformation beruhen
Organisation
- Sichere Arbeitsverfahren
- Überwachung
- Betriebserlaubnis
Bereitstellung und Anwendung zusätzlicher Schutzeinrichtungen 4)
Anwendung persönlicher Schutzausrüstungen
Ausbildung, usw.
Restrisiko nach Ausführung aller Schutzmaßnahmen

Bild 2/2
Prozess der Risikominderung

dem Maschinenkonstrukteur helfen, eine sichere Maschine zu konstruieren. Inhärente Sicherheit der Maschine ist das erste Ziel. Erst gegen dann noch verbleibende Gefährdungen sind Schutzabsperrungen vorzusehen (siehe ISO 12100-2 Kap. 4). Geeignete Implementierung sicherheitsrelevanter Steuerungsfunktionen ist ein wesentlicher Beitrag zur inhärenten Sicherheit (siehe ISO 12100-2 Abschnitt 4.11). Für Steuerungen, die programmierbare elektronische Komponenten enthalten, wird auf IEC 61508 verwiesen.

Für viele Maschinentypen gibt es C-Normen, in denen notwendige

Maßnahmen zur Risikoreduzierung, bereits festgelegt sind. Sie definieren notwendige Schutzmaßnahmen mit der zugehörigen Safety Performance , d.h. den erforderlichen Kategorien für die sicherheitsrelevanten Teile der Steuerung.

Um der technischen Entwicklung Rechnung zu tragen oder wenn keine C-Norm vorhanden ist, ist es in vielen Fällen notwendig bei der Konstruktion einer Maschine diesen Prozess erneut durchzuführen und die zu realisierenden Maßnahmen der Risikominderung gemäß dem aktuellen Stand der Technik festzulegen.

Mit der Spezifikation der Sicherheitsanforderungen legt der Maschinenkonstrukteur die Anforderungen an die Steuerung und die Schutzeinrichtungen fest. Diese Spezifikation beinhaltet die genaue Beschreibung der einzelnen Sicherheitsfunktionen und deren erforderliche Safety Performance.

Bestimmung notwendiger Maßnahmen zur Risikominderung

Für viele Maschinentypen gibt es spezifische C-Normen, in denen die notwendigen Schutzmaßnahmen bereits festgelegt sind. Der Maschinenhersteller kann diese Normen anwenden, wenn sie für die betrachtete Maschine zutreffen und darf dann vermuten (siehe Kapitel 1 „Vermutungswirkung"), dass die Sicherheitsziele der EU-Maschinenrichtlinie erfüllt sind.
In diesem Fall sind für die sicherheitsrelevanten Steuerungsfunktionen auch die notwendigen Kategorien nach EN 954 vorgegeben.

Entspricht die vorgesehene technische Realisierung der betrachteten Maschine den Vorgaben der C-Norm, brauchen die im Folgenden beschriebenen Schritte der Risikoanalyse nicht erneut durchgeführt zu werden. Die Sicherheitsfunktionen und deren Safety Performance, d.h. erforderliche Kategorie, sind durch die C-Norm vorgegeben.
Werden zur Realisierung der Sicherheitsfunktionen komplexe elektronische Geräte, z.B. Sicherheits-SPS eingesetzt, ist die angegebene Kategorie allerdings nicht direkt anwendbar.
Die mit den Kategorien von EN 954 verbundenen Anforderungen reichen alleine nicht aus. Programmierbare Steuerungen für Sicherheitsaufgaben müssen IEC 61508 erfüllen. Um die mit einer bestimmten Kategorie verbundenen Schutzziele zu erfüllen, muss die programmierbare Steuerung den gemäß Bild 2/3 zugeordneten SIL erreichen.

Weicht die Maschinenkonstruktion von den Vorgaben der C-Norm ab, um z.B. die neuen Möglichkeit der elektronischen Sicherheitssteuerungen oder Sicherheitsantriebsfunktionen zu nutzen, muss eine Risikoanalyse durchgeführt werden und es muss die für die neue Technik angemessene Safety Performance (Fußnote 2) bestimmt werden.

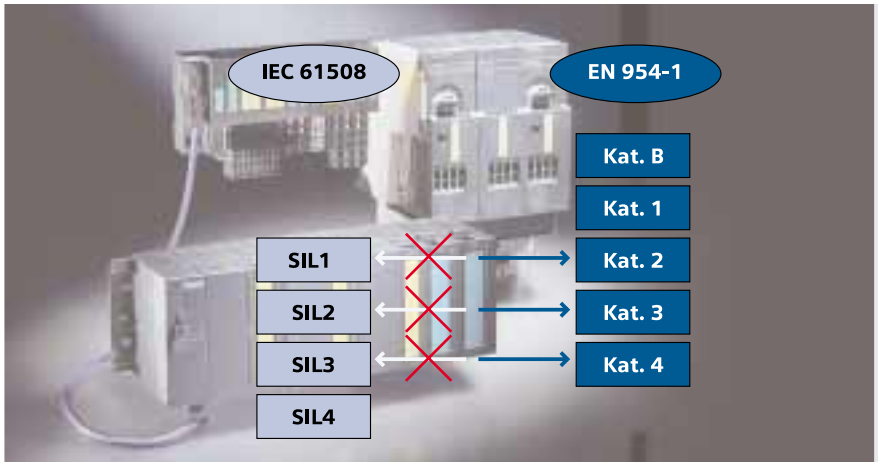


Bild 2/3
Notwendiger SIL zur Erfüllung bestimmter Kategorien

Abgrenzung der betrachteten Maschine

Die Konstruktion der Maschine beginnt mit der Festlegung ihrer Grenzen. Diese umfassen:

- Verwendungsgrenzen:
  Das ist die Festlegung der bestimmungsgemäßen Verwendung einschließlich der verschiedenen Betriebsarten, Benutzungsphasen und unterschiedlichen Eingriffsmöglichkeiten für die Benutzer, sowie vernünftigerweise vorhersehbarer Missbrauch.

- räumliche Grenzen:
  (z.B. Bewegungsraum, Platzbedarf für Installation und Wartung, Schnittstellen „Operator/Maschine" und „Maschine/Energiezufuhr")

- Umgebungsgrenzen:
  Grenzwerte der Umgebungsbedingungen, z.B. Temperatur, Feuchte

- zeitliche Grenzen:
  Festlegung der vorhersehbaren „Lebensdauergrenze" der Maschine unter Berücksichtigung ihrer bestimmungsgemäßen Verwendung und/oder einiger ihrer Teile (z.B. Werkzeuge, Verschleißteile, elektrische Bauteile).

Identifizierung möglicher Gefährdungen (Hazards)

Nachdem die Grenzen der betrachteten Maschine festgelegt sind, sind alle möglichen Gefährdungen, die von dieser Maschine ausgehen können, zu identifizieren. (Kapitel 4 von ISO 12100-1 enthält eine Auflistung möglicher, zu betrachtender Gefährdungen.)

Bei der Identifizierung möglicher Gefährdungen (Hazards) ist auch zu untersuchen, ob Funktionsfehler oder Ausfälle der Steuerung, der Regeleinrichtungen oder vorhandener Schutzeinrichtungen zu Gefährdungen führen können. Das mögliche Fehlverhalten (z.B. die Steuerung erzeugt ein Ein-Signal obwohl ein Aus-Signal ausgegeben und beibehalten werden soll) ist bezüglich seiner Wirkung auf die Maschine und deren Schutzeinrichtungen zu betrachten. Dabei braucht nicht untersucht zu werden, welche „internen" Ursachen in den betrachteten Geräten zu der Fehlfunktion führen können.

Für jeden möglichen Funktionsfehler ist zu untersuchen, welche Gefährdungen daraus resultieren können. Zum Beispiel ist zu prüfen,

- ob ein beliebiger Fehler oder eine Kombination von Fehlern in der Steuerung zu einer gefährlichen (Fehl-)Funktion der Maschine (z.B. unbeabsichtigter Anlauf) führen kann,

- ob bei der Verwendung drehzahlveränderbarer Antriebe Abweichungen von der Sollgeschwindigkeit Gefahren verursachen können.

- ob das Versagen eines Operatorkommandos (z.B. Stop-Kommando) zu einer Gefährdung führen kann

Bei der Risikoanalyse ist zunächst immer von einer „worst case" Betrachtung auszugehen, d.h. es muss unterstellt werden, dass Funktionsfehler auftreten können. Hat die Untersuchung ergeben, dass ein Funktionsfehler eine Gefährdung verursachen kann, dann ist diese Funktion sicherheitsrelevant und es muss eine Risikobewertung gemacht werden. Abhängig vom Ergebnis der Risikobewertung sind Maßnahmen zur Risikoreduzierung notwendig.

[2] Der Begriff „Safety Performance" wird hier als übergeordneter Begriff für die sicherheitsbezogenen Leistungsfähigkeit der Steuerung verwendet. Er umfasst die in den verschiedenen Normen verwendeten Begriffe „Kategorie", „Safety Integrity" und „Performance Level".

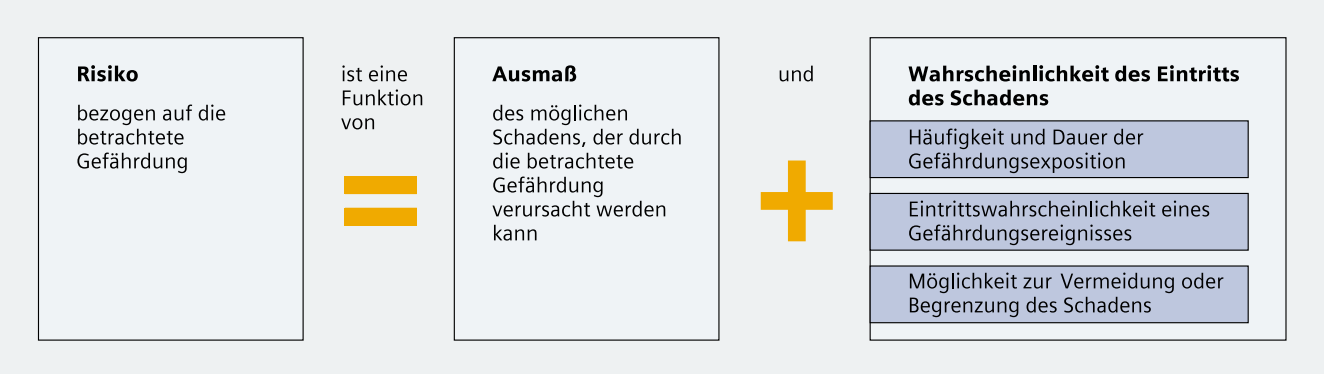

Risiko
bezogen auf die betrachtete Gefährdung
ist eine Funktion von
Ausmaß
des möglichen Schadens, der durch die betrachtete Gefährdung verursacht werden kann
und
Wahrscheinlichkeit des Eintritts des Schadens
Häufigkeit und Dauer der Gefährdungsexposition
Eintrittswahrscheinlichkeit eines Gefährdungsereignisses
Möglichkeit zur Vermeidung oder Begrenzung des Schadens

Bild 2/4
Elemente der Risikobewertung

Risikoabschätzung und Risikobewertung

Siehe dazu auch EN 1050 Kap. 7 und 8.

Für alle zuvor identifizierten Hazards müssen die damit verbundenen Risiken bewertet werden. Übersteigt das Risiko einer bestimmten Gefährdung das tolerierbare Maß, sind Maßnahmen zur Risikoreduzierung notwendig.

Hinweis: Das Ergebnis der Bewertung sollte für jede einzelne Gefährdung dokumentiert werden.

Ein Risiko entsteht durch Zusammenwirken verschiedener Ursachen (siehe Bild 2/4).

- Schwere des möglichen Schadens
- Häufigkeit mit der sich Personen im Gefahrenbereich aufhalten
- Wahrscheinlichkeit, dass das gefährliche Ereignis eintritt
- Möglichkeit den Schaden zu vermeiden oder zu mindern

Seine Höhe kann durch Bewertung dieser Elemente abgeschätzt werden.

Risikoreduzierung

Falls das abgeschätzte Risiko zu hoch erscheint, muss es vermindert werden. Dazu muss zuerst durch Konstruktionsänderung versucht werden, die Maschine sicher zu machen (siehe Maschinenrichtlinie Anhang I (1) 1.1.2 und ISO 12100-1 Kap. 5.4.) Falls das nicht möglich ist, muss durch geeignete Schutzmaßnahmen eine Risikominderung erreicht werden.

- Die Schwere eines möglichen Schadens kann z.B. dadurch verringert werden, dass während der Anwesenheit von Personen die Bewegungsgeschwindigkeiten oder Kräfte der Maschinenteile verringert werden.

- Durch Absperreinrichtungen kann die Häufigkeit, mit der Personen im Gefahrenbereich sind, verringert werden.

- Es besteht immer eine gewisse Wahrscheinlichkeit, dass sich eine Maschine nicht bestimmungsgemäß verhält oder Schutzeinrichtungen versagen. Dies kann durch Fehler in beliebigen Teilen der Maschine verursacht werden. Eine Minderung dieses Risikofaktors kann durch geeignete Konstruktion der sicherheitsrelevanten Teile erreicht werden. Zu den sicherheitsrelevanten Teilen gehört auch die Steuerung der Maschine, wenn durch deren Versagen eine Gefährdung entstehen kann. Durch Realisierung der Steuerung gemäß IEC 62061 kann das Risiko, das durch Fehler der Steuerung verursacht wird, vermindert werden.

- Die Möglichkeit einen Schaden zu vermeiden kann u.a. dadurch vergrößert werden, dass Gefahrenzustände rechtzeitig erkennbar sind, z.B. durch Signallampen.

Ein gemeinsamer Parameter all dieser Elemente ist die Wahrscheinlich des Eintretens eines unerwünschten Ereignisses. Durch Vermindern dieser Wahrscheinlichkeit kann eine Verminderung des Risikos erreicht werden (siehe Bild 2/5).

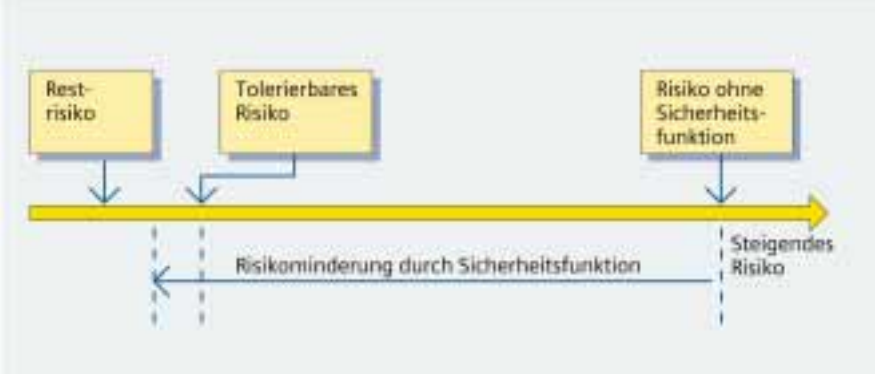


Bild 2/5
Risikominderung

Maßnahmen zur Risikoreduzierung

Das Konzept der Risikobeurteilung orientiert sich an den möglichen Gefährdungen. Es verlangt, dass für jede identifizierte Gefährdung geeignete Maßnahmen zu deren Beseitigung getroffen werden. Oder falls das nicht möglich ist, deren Eintretenswahrscheinlichkeit ausreichend reduziert wird.

Sicherheitsrelevante Steuerungsfunktionen

Hat die Risikoeinschätzung ergeben, dass eine Gefährdung aufgrund möglicher Funktionsfehler der Steuerung verursacht wird, kann dieses Risiko dadurch verringert werden, dass die Wahrscheinlichkeit gefährlicher Fehler der Steuerung ausreichend reduziert wird.

Solche Situationen sind z.B. dann gegeben, wenn eine Maschine für Wartungs- oder Einrichtarbeiten angehalten oder ihre Geschwindigkeit verringert wird, um dem Personal gefahrloses Arbeiten an der Maschine zu ermöglichen. Hier kann durch unerwarteten Anlauf oder plötzliche Beschleunigung, z.B. wegen eines Steuerungsfehlers, eine Gefährdung entstehen.

Wenn für bestimmte Tätigkeiten zum Schutz des Bedieners der Bewegungsbereich begrenzt wird, so kann ein Versagen dieser Begrenzung zu einer Gefährdung führen.

Die Versagenswahrscheinlichkeit dieser Funktionen muss also ausreichend gering sein, um das Risiko auf ein tolerierbares Maß zu begrenzen.

Beispiel (1) sicherheitsrelevante Steuerungsfunktion

Maschine mit mehreren bewegten Teilen (Achsen). Verletzungsgefahr besteht aufgrund der Bewegung jedes dieser Teile. Zu Instandsetzungsarbeiten muss der Bediener in den Gefahrenbereich, aber die Maschine soll nicht vollständig abgeschaltet werden, weil dadurch Schäden am Produkt entstehen (können).

Während der Instandsetzung wird zum Schutz des Bedieners und des Produktes die Bewegungsgeschwindigkeit auf ungefährliches Niveau begrenzt bzw. bestimmte Teile der Maschine in definierter Position gehalten. Das Einhalten der Geschwindigkeitsgrenzen und Positionen ist sicherheitsrelevant. Ein Versagen der betreffenden Steuerungsfunktion kann zu einer Gefährdung des Bedieners führen (z.B. durch unerwartete Beschleunigung, Einengung / Quetschung bei Verlassen der Position)

Die Sicherheitsfunktion ist in diesem Fall: „Begrenzen der Geschwindigkeit bestimmter Maschinenteile und Einhalten eingestellter Positionen bestimmter Maschinenteile. Falls ein Grenzwert, z.B. wegen einer Störung, überschritten wird, ist der betreffende Antrieb abzuschalten und eine mechanische Bremse auszulösen."

Für diese Situation muss eine Risikobewertung gemacht werden, um die notwendige Safety Performance der Sicherheitsfunktion zu ermitteln.

Schutzabsperrungen

Hat die Risikoeinschätzung ergeben, dass Schutzabsperrungen notwendig sind, die den Zugang zum Gefahrenbereich verhindern, dann müssen diese Maßnahmen so ausgeführt werden, dass ihr Versagen ausreichend unwahrscheinlich ist. Absperrungen müssen an allen Zugangsstellen überwacht werden, so dass bei eingeschalteter Maschine kein Zugang zum Gefahrenbereich möglich ist. Neben diesen Maßnahmen, die den Zugang von Personen einschränken, kann es auch notwendig sein, den Bewegungsbereich von Maschinen oder Emissionen zu begrenzen. Der Aufenthaltsbereich von Personen (siehe Bild 2/6) muss geschützt werden, indem z.B. verhindert wird, dass Teile der Maschine in diesen Bereich hineinragen.

Beispiel (2) sicherheitsrelevante Schutzabsperrung

Im Arbeitsbereich einer Maschine (Fertigungszelle) darf sich während der Produktion keine Person aufhalten, da wegen der schnellen und zum Teil unerwarteten Bewegungen der Maschine hohe Verletzungsgefahr besteht. Die Maschine darf deshalb nur im Produktionsbetrieb laufen, wenn durch Absperren und Verriegeln aller Zugangsmöglichkeiten gewährleistet ist, dass keine Personen in den Gefahrenbereich gelangen können.

Die Sicherheitsfunktion ist in diesem Fall: „Während des Produktionsbetriebes alle Zugänge zum Arbeitsbereich der Maschine (Fertigungszelle) verriegeln. Falls ein Fehler z.B. in einer Verriegelung festgestellt wird, so dass ein unerlaubter Zugang zur Maschine nicht mehr ausgeschlossen werden kann, muss die Maschine angehalten werden."

Für diese Situation muss eine Risikobewertung gemacht werden, um die notwendige Safety Performance der Sicherheitsfunktion zu ermitteln.

Zur Beseitigung oder Verminderung des Risikos jeder identifizierten Gefährdung werden sicherheitsrelevante Steuerungsfunktionen definiert. Damit diese Funktionen die gewünschte Risikoreduzierung erreichen, müssen sie eine ausreichende Safety Performance haben. Die notwendige Safety Performance jeder Funktion muss für die durch sie zu beseitigende Gefährdung ermittelt werden.

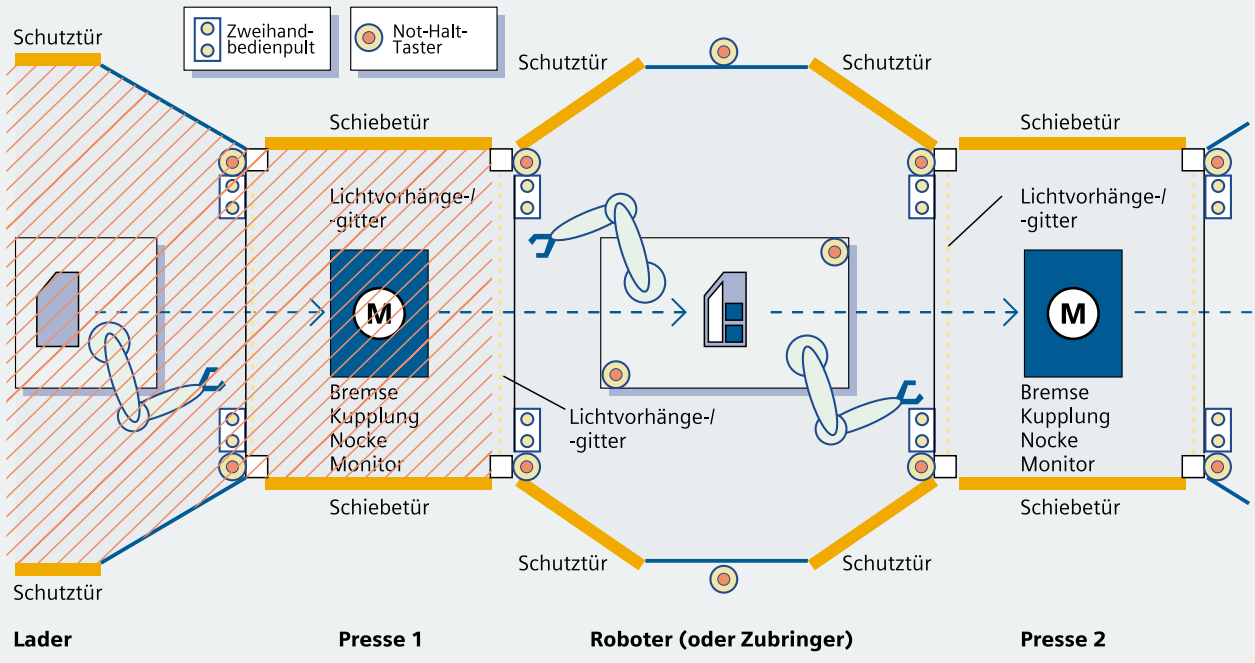


Bild 2/6
Gefahrenbereiche einer integrierten Maschine

2.3 Hängt die Schutzmaßnahme von einer Steuerung ab?

Risikoelemente nach EN 1050 (ISO 14121)

Die Risikobeurteilung nach EN 1050 erlaubt die Bestimmung des Risikos mittels der vier Risikoelemente:

- Schwere des möglichen Schadens
- Häufigkeit mit der sich Personen im Gefahrenbereich aufhalten
- Wahrscheinlichkeit, dass das gefährliche Ereignis eintritt
- Möglichkeit den Schaden zu vermeiden oder zu mindern

Diese Risikoelemente wiederum bilden die Eingangsparameter zur Realisierung einer sicherheitsrelevanten Steuerungsfunktion: sie ermöglichen erst die Zuordnung des Risikos an die Anforderungen der sicherheitsgerichteten Steuerung.

Deshalb bieten sowohl die EN 954-1 also auch die IEC 62061 durch jeweilige Verfahren zur Bewertung der Risikoelemente und Einstufung der Safety Performance an.

Ermittlung der notwendigen Safety Performance (Safety Integrity)

Wurde bei der Risikountersuchung festgestellt, dass Funktionsfehler der Steuerung oder das Versagen von Schutzeinrichtungen zu einem zu hohen Risiko führen können, dann muss deren Wahrscheinlichkeit soweit verringert werden bis das verbleibende Risiko tolerierbar ist. D.h. die Steuerung muss eine ausreichende „Safety Performance " erreichen.

Zur Beantwortung der Frage was als ausreichend sicher angenommen werden kann, wird bisher meistens das in Anhang B von EN 954-1 / ISO 13849-1 beschriebene Verfahren (Risikograph) angewendet und damit bestimmte „Kategorien" für die sicherheitsrelevanten Steuerungsfunktionen ermittelt.

Mit IEC 62061 gibt es nun neben der EN 954 eine neue Norm für sicherheitsrelevante Maschinensteuerungen. In dieser Norm wird ein Verfahren beschrieben, das eine an Wahrscheinlichkeiten orientierte quantifizierte und damit hierarchische Abstufung der Safety Performance verwendet. Das Ergebnis der Risikoanalyse ist dann der Safety Integrity Level (SIL) für die betreffenden Sicherheitsfunktionen.

Mit ihrer Neufassung wird auch in der ISO 13849-1 eine ähnliche quantifizierte und damit hierarchische Abstufung der Safety Performance eingeführt. Das dort als Performance Level (PL) bezeichnete Maß korreliert über die zugeordneten Ausfallwahrscheinlichkeiten mit den SILs der IEC 62061.

Die Verfahren beider Normen basieren auf den gleichen Prinzipien. Es wird deshalb dem Anwender überlassen, welche Norm er anwendet. Die zuständigen technischen Komitees von IEC und ISO empfehlen die in der folgenden Tabelle (Bild 2/11) angegebene Auswahl.

Hinweis: Falls für den betrachteten Maschinentyp eine C-Norm existiert, sind vorrangig die dort beschriebenen Schutzmaßnahmen mit den angegebenen Kategorien zu realisieren. Die Vorgaben sollten aber auf ihre Aktualität bezüglich neuerer technischer Entwicklungen geprüft werden.

Safety Performance für Realisierung der Steuerung nach EN 954

In der EN 954-1 ist ein Verfahren zur Bestimmung der bei einem bestimmten Risiko notwendigen Kategorie beschrieben. Da die Kategorien nicht hierarchisch sind, ist der im Bild 2/7 dargestellte Risikograph nur eine Empfehlung. Das Verfahren lässt außerdem zu, dass für ein bestimmtes Risiko unterschiedliche Kategorien ausgewählt werden können. Das Ergebnis ist nicht eindeutig und kann außerdem von der zu verwendenden Lösungstechnologie beeinflusst werden.

[3] In den verschiedenen Normen ist das Maß für die „Safety Performance" unterschiedlich definiert: Kategorien in EN 954, Safety Integrity Level (SIL) in IEC/EN 61508 und IEC 62061 und Performance Level (PL) in draft ISO 13849-1(rev).

[4] Der Begriff „Safety Performance" wird hier als übergeordneter Begriff für die sicherheitsbezogenen Leistungsfähigkeit der Steuerung verwendet. Er umfasst die in den verschiedenen Normen verwendeten Begriffe „Kategorie", „Safety Integrity" und „Performance Level".

Verfahren zur Bewertung der Risikoelemente und Einstufung der Safety Performance.

Risikograph nach EN 954

Ziel ist es, eine geforderte Kategorie durch die Risikoelemente zu ermitteln.

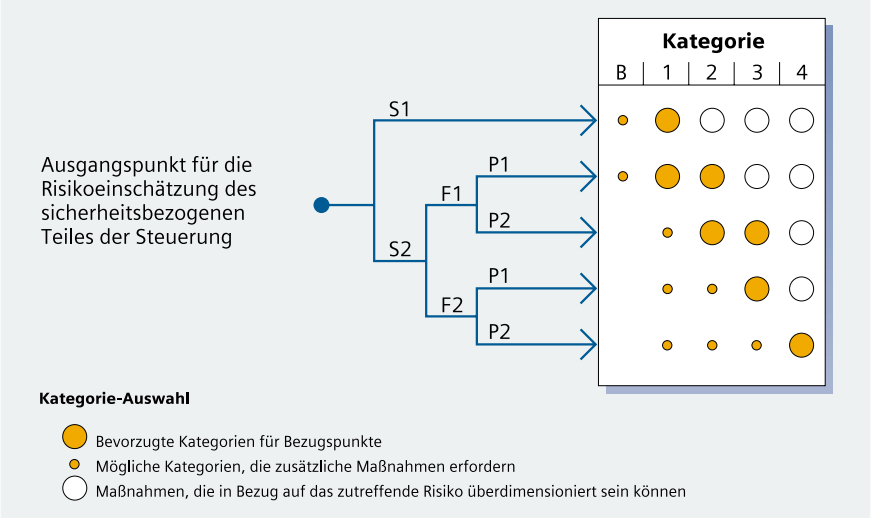


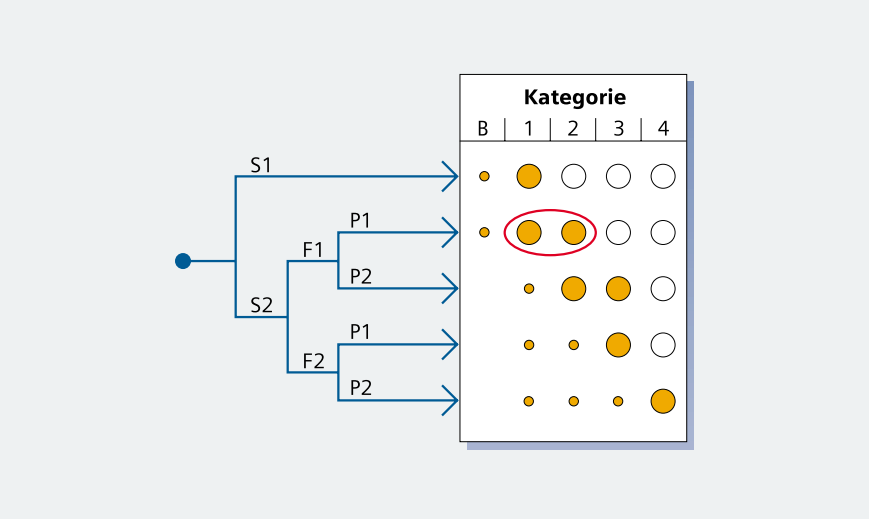
Bild 2/7
Risikograph zur Bestimmung erforderlicher Kategorien aus EN 954-1

Erläuterungen zur Interpretation des Risikographen nach EN 954

Beispiel 1:

Die Risikobeurteilung führt über S2 (schwere irreversible Verletzung einer oder mehrerer Personen oder Tod einer Person), F1 (selten bis öfter) und P1 (möglich unter bestimmten Bedingungen) zu einer erforderlichen Kategorie 1 oder 2.

Die Kategorie 2 stellt dabei keine bessere „Widerstandsfähigkeit" gegenüber einem Fehler dar (ein Fehler führt zum Verlust der Sicherheitsfunktion), jedoch wird die Fehleraufdeckung im Vergleich zu Kategorie 1 verbessert

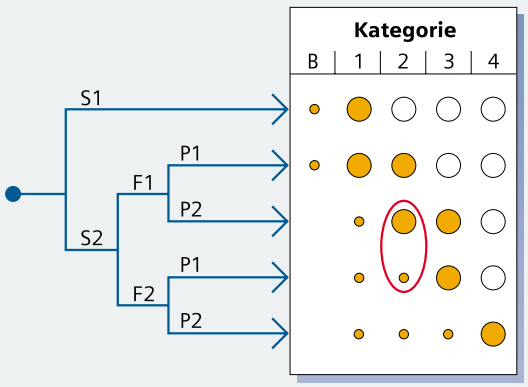


[5] EN 954 heißt international ISO 13849.

Beispiel 2:

Die Sicherheit („Widerstandsfähigkeit" gegenüber Fehlern) kann durch zusätzliche Maßnahmen erhöht werden, aber bei gleich bleibender Kategorie.

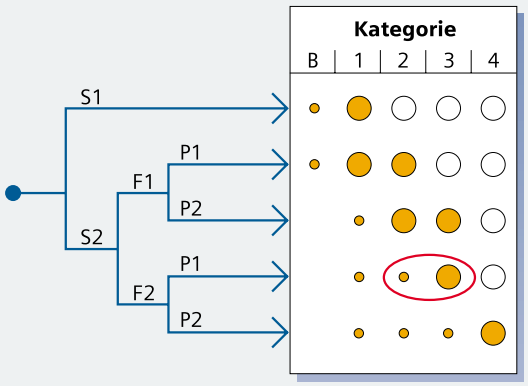
In diesem Beispiel ist die erreichte Kategorie nach wie vor die Kategorie 2.



Beispiel 3:

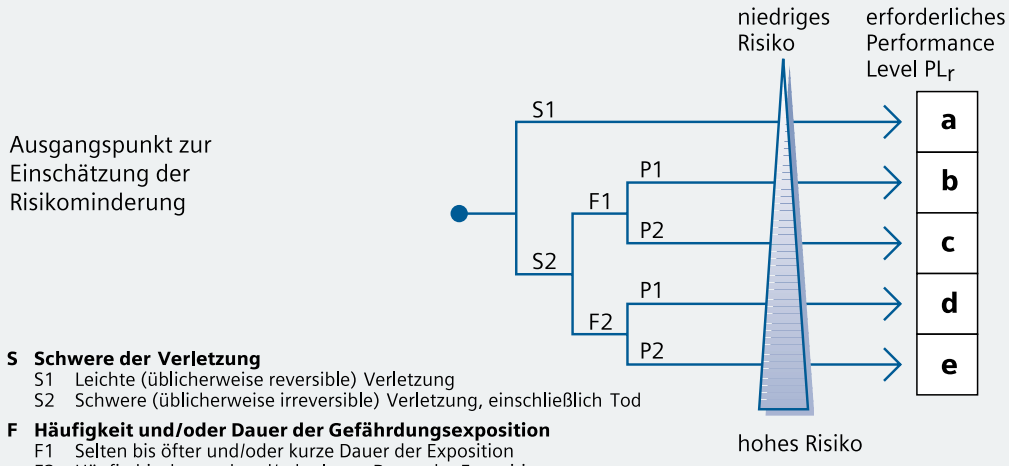
Die geforderte Kategorie 3 kann nicht durch Zusatzmaßnahmen mit einer anderen Kategorie (hier mit der Kategorie 2) erreicht werden.
In diesem Beispiel wird zwar das gleiche Risiko abgedeckt (die gleiche „Safety Performance" erreicht), jedoch verlangt die Risikobeurteilung nach wie vor eine Kategorie 3 zur Risikominderung.

Mit der vorgesehenen Neufassung der EN 954-1 als ISO 13849-1(rev) wird dort ein hierarchisch abgestuftes quantifiziertes Maß für die Safety Performance, bezeichnet als Performance Level (PL) eingeführt (siehe Bild 2/8). Damit werden die Mehrdeutigkeiten bei der Auswahl der Kategorien beseitigt.



Risikograph nach prEN ISO 13849-1

Ziel ist es einen geforderten Performance Level PL_r, also die Wahrscheinlichkeit gefahrbringender Ausfälle des Systems, durch die Risikoelemente zu ermitteln.



S Schwere der Verletzung
S1 Leichte (üblicherweise reversible) Verletzung
S2 Schwere (üblicherweise irreversible) Verletzung, einschließlich Tod

F Häufigkeit und/oder Dauer der Gefährdungsexposition
F1 Selten bis öfter und/oder kurze Dauer der Exposition
F2 Häufig bis dauernd und/oder lange Dauer der Exposition

P Möglichkeit zur Vermeidung der Gefährdung
P1 Möglich unter bestimmten Bedingungen
P2 Kaum möglich

a, b, c, d, e = Ziele von safety-related Performance Level

Bild 2/8
Risikograph (Entwurf) nach ISO 13849-1 (rev) zur Bestimmung der erforderlichen Performance Level

Die Performance Level (PL) sind ein quantitatives Maß für die Safety Performance genauso wie die Safety Integrity Level (SIL) in IEC 61508 und IEC 62061. Den Zusammenhag zwischen beiden Parametern zeigt das Bild 2/9.

Die somit scheinbar entstandene Vielfalt erscheint zunächst verwirrend. Es bestehen aber definierte Beziehungen zwischen den verschiedenen Maßen der geforderten Safety Performance.

Für die Zuordnung der geforderten Kategorien zu geforderten Performance Levels oder Safety Integrity Levels gibt es von den zuständigen Gremien noch keine offizielle Festlegung. Auf Basis gleicher Risikoparameter kann

[6] Der dargestellte Risikograph ist ein Entwurf, der in den zuständigen Gremien noch diskutiert wird.

Performance level PL	Mittlere Wahrscheinlichkeit gefahrbringender Ausfälle innerhalb einer Stunde	SIL EN 61508-1 (IEC 61508-1) zur Information
a	≥ 10-5 to < 10-4	Keine speziellen Sicherheitsanforderungen
b	≥ 3x 10-6 to < 10-5	1
c	≥ 10-6 to < 3x10-6	1
d	≥ 10-7 to < 10-6	2
e	≥ 10-8 to < 10-7	3

Anmerkung 1:
Die Darstellung für jede Gefahrensituation wird in fünf Stufen von a bis e unterteilt. Dabei ist die Risikoreduzierung bei a am niedrigsten, bei e am höchsten.
Anmerkung 2:
Die Performance Level b und c zusammen decken nur eine Größenordnung der mittleren Wahrscheinlichkeit für gefahrbringende Ausfälle ab (ebenso auf der SIL Skala).

Bild 2/9
Performance Level

aus den Risikographen in den Bildern 2/7 und 2/8 folgende Zuordnung vorgenommen werden:

Kategorie 1 → PL_r b → SIL 1
Kategorie 2 → PL_r c → SIL 1
Kategorie 3 → PL_r d → SIL 2
Kategorie 4 → PL_r e → SIL 3

Diese Zuordnung einer geforderten Kategorie zum geforderten PL_r bzw. SIL ist als Vereinfachung zu betrachten. Im Einzelfall sollten wegen der Mehrdeutigkeit bei den Kategorien die Besonderheiten der jeweiligen Anwendung beachtet werden.

Safety Performance für Realisierung der Steuerung nach IEC 62061

Das in IEC 62061 im Anhang A beschriebene Verfahren basiert ebenfalls auf den in EN 1050 definierten Risikoparametern, verwendet jedoch im Gegensatz zur ISO 13849-1 ein tabellarisches Verfahren, das direkt zur Dokumentation der durchgeführten Risikobewertung und SIL Zuweisung verwendet werden kann.

Für die einzelnen Risikoparameter ist anhand der im Kopf der Tabelle vorgegebenen Werte die zugehörige Gewichtung auszuwählen. Die Summe der Gewichte aller Parameter ergibt die Wahrscheinlichkeitsklasse des Schadens.

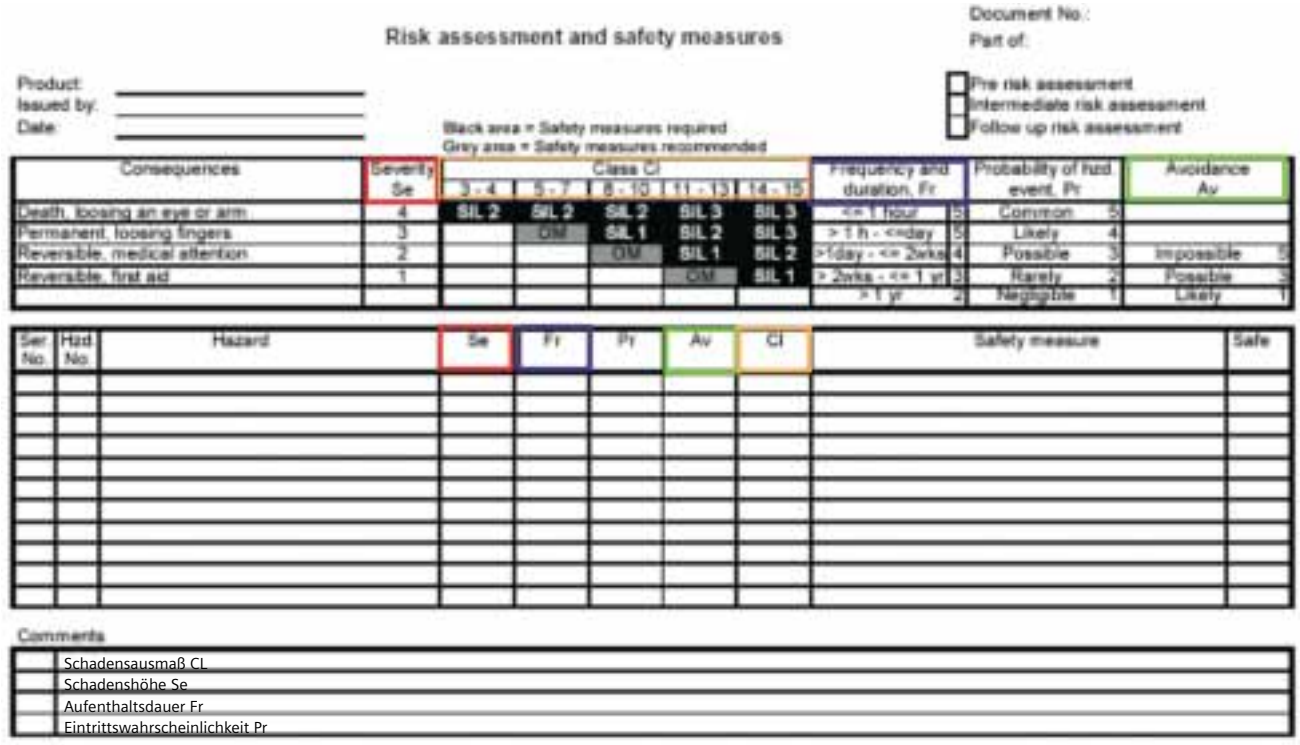
Cl = Fr + Pr + Av

Siehe Erläuterung zu Bild 2/10.

Mit Hilfe dieser Wahrscheinlichkeitsklasse und der möglichen Schadensschwere der betrachteten Gefährdung kann dann aus der Tabelle der notwendige SIL für die zugehörige Sicherheitsfunktion abgelesen werden.

Tabelle zur Bestimmung des Sicherheits Integritäts Level nach IEC 62061 (SIL-assignment)

Ziel ist es einen geforderten Sicherheits-Integritätslevel SIL, also die Wahrscheinlichkeit gefahrbringender Ausfälle des Systems, durch die Risikoelemente zu ermitteln.



Risk assessment and safety measures

Document No.:
Part of:

Product:
Issued by:
Date:

☐ Pre risk assessment
☐ Intermediate risk assessment
☐ Follow up risk assessment

Black area = Safety measures required
Grey area = Safety measures recommended

Consequences	Severity Se	Class Cl 3 - 4	5 - 7	8 - 10	11 - 13	14 - 15	Frequency and duration, Fr		Probability of hzd event, Pr		Avoidance Av	
Death, loosing an eye or arm	4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3	<= 1 hour	5	Common	5		
Permanent, loosing fingers	3		OM	SIL 1	SIL 2	SIL 3	> 1 h - <=day	5	Likely	4		
Reversible, medical attention	2			OM	SIL 1	SIL 2	>1day - <= 2wks	4	Possible	3	Impossible	5
Reversible, first aid	1				OM	SIL 1	> 2wks - <= 1 yr	3	Rarely	2	Possible	3
							> 1 yr	2	Negligible	1	Likely	1

Ser. No.	Hzd. No.	Hazard	Se	Fr	Pr	Av	Cl	Safety measure	Safe

Comments

	Schadensausmaß CL
	Schadenshöhe Se
	Aufenthaltsdauer Fr
	Eintrittswahrscheinlichkeit Pr

Bild 2/10
Beispielformular für SIL Maßnahmen

2.4 Spezifikation der Sicherheitsanforderungen

Wurden Steuerungsfunktionen als sicherheitsrelevant identifiziert oder sollen Schutzmaßnahmen mit Mitteln der Steuerung realisiert werden, sind die genauen Anforderungen für diese „Sicherheitsfunktionen“ („sicherheitsrelevanten Steuerungsfunktionen“) in der Spezifikation der Sicherheitsanforderungen („safety requirements specification") festzulegen. Diese Spezifikation beschreibt für jede sicherheitsrelevante Funktion u.a.:

- deren Funktionalität, d.h. alle erforderlichen Eingangsinformationen, deren Verknüpfung und die zugehörigen Ausgangszustände oder Aktionen, sowie die Benutzungshäufigkeit
- die notwendigen Reaktionszeiten
- die geforderte Safety Performance

Die Spezifikation der Sicherheitsanforderungen enthält alle Information, die für den Entwurf und die Implementierung der Steuerung notwendig ist. Sie ist die Schnittstelle zwischen Maschinenkonstrukteur und Hersteller / Integrator der Steuerung und kann so auch zur Abgrenzung von Verantwortlichkeiten dienen.

Entwurf und Realisierung der sicherheitsrelevanten Steuerungen

Welche Norm ist anzuwenden, ISO 13849 oder IEC 62061?

Eine sicherheitsrelevante Steuerung für Maschinen kann sowohl nach IEC 62061 als auch nach ISO 13849 realisiert werden. Mit den Anforderungen jeder der beiden Normen werden die Sicherheitsziele der Maschinenrichtlinie bezüglich funktionaler Sicherheit erfüllt. Eine Entscheidungshilfe für die Auswahl der anzuwendenden Norm gibt die folgende Tabelle, die als Empfehlung im Vorwort beider Normen steht.

	Technologie zur Ausführung von sicherheitsrelevanten Steuerungsfunktionen	EN ISO 13849-1(rev.)	IEC 62061
A	Nicht-elektrisch, z.B. Hydraulik	X	nicht abgedeckt
B	Elektromechanik, z.B. Relais und/ oder einfache Elektronik	Beschränkt auf vorgesehene Architekturen (siehe Anmerkung 1) und maximal bis PL = e	Alle Architekturen und maximal bis SIL 3
C	Komplexe Elektronik, z.B. programmierbare Elektronik	Beschränkt auf vorgesehene Architekturen (siehe Anmerkung 1) und maximal bis PL = d	Alle Architekturen und maximal bis SIL 3
D	A kombiniert mit B	Beschränkt auf vorgesehene Architekturen (siehe Anmerkung 1) und maximal bis PL=e	X siehe Anmerkung 3
E	C kombiniert mit B	Beschränkt auf vorgesehene Architekturen (siehe Anmerkung 1) und maximal bis PL = d	Alle Architekturen und maximal bis SIL 3
F	C kombiniert mit A, oder C kombiniert mit A und B	X siehe Anmerkung 2	X siehe Anmerkung 3

"X" zeigt, dass der Punkt von dieser Norm abgedeckt wird.

Anmerkungen

1 Vorgesehene Architekturen sind im Anhang B der EN ISO 13849-1 beschrieben und geben einen vereinfachten Ansatz für die Quantifizierung.

2 Für komplexe Elektronik: Verwendung vorgesehener Architekturen in Übereinstimmung mit der EN ISO 13849-1 bis PL = d oder jede Architektur in Übereinstimmung mit IEC 62061.

3 Für nicht elektrische Technologien: Verwenden Sie Teile, die der EN ISO 13849-1 (rev) entsprechen, als Subsysteme.

Bild 2/11
Empfohlene Anwendung von IEC 62061 & ISO 13849-1 (rev.)

Hinweis:

Die IEC 62061 wurde September 2004 als IS angenommen. Von der ISO 13849-1 (rev) wurde in 2004 der Entwurf prEN ISO 13849-1 (bzw. DIS ISO 13849-1) zur Kommentierung veröffentlicht. Aufgrund der eingegangenen Kommentare sind noch Änderungen zu erwarten, bevor die ISO 13849-1 zum abschließenden Voting veröffentlicht werden kann. Eine endgültige Fassung wird frühestens Ende 2005 erwartet.

Formal ist derzeit (Anfang 2005) nur die EN 954-1 unter der Maschinenrichtlinie harmonisiert und insofern die verbindliche Norm zur Erfüllung der EU-Maschinenrichtlinie. Bei Anwendung der IEC 62061 werden jedoch die Anforderungen der EN 954-1 erfüllt und darüber hinaus auch der aktuelle Stand der Technik für programmierbare elektronische Systeme einschließlich Buskommunikation.

Der Entwurf der ISO 13849-1 behandelt wie auch die EN 954-1 verschiedene Technologien, wie z.B. elektrisch, hydraulisch, pneumatisch und mechanisch.

Ziel ist es auf Basis „vorgesehener Architekturen“ und einer entsprechenden Kategorie eine sicherheitsgerichtete Steuerungsfunktion realisieren zu können: dies spiegelt die heutigen praktizierten Realisierungsansätze wieder.

Zu einer sicherheitsgerichteten Software werden keine Aussagen getroffen. Es wird hier dagegen explizit auf andere Normen verwiesen (in der IEC 62061 z.B. wird das Thema Software ausführlich behandelt).

2.5 Entwurf und Realisierung der (sicherheitsrelevanten) Steuerung nach IEC 62061

Zielsetzung: Ein sicherheitsrelevantes (Steuerungs-) System muss eine Sicherheitsfunktion korrekt ausführen. Auch im Fehlerfall muss sie sich so verhalten, dass die Maschine oder Anlage in einen sicheren Zustand bleibt oder gebracht wird.

Ermittlung der notwendigen Safety Performance (Safety Integrity)

Siehe dazu Kapitel 2.3 „Hängt die Schutzmaßnahme von einer Steuerung ab?“

Philosophie/Theorie

Strukturierungsprinzip für ein sicherheitsrelevantes Steuerungssystem

Wesentliche Voraussetzung für das korrekte und bestimmungsgemäße Funktionieren einer Steuerung ist deren korrekte Konstruktion. Um dieses Ziel zu erreichen hat IEC 62061 einen systematischen top down Entwurfsprozess definiert:

Ein sicherheitsrelevantes elektrisches Steuerungssystem (Safety related electrical control system, SRECS) umfasst alle Komponenten von der Informationserfassung über die Informationsverknüpfung bis einschließlich der Ausführung von Aktionen. Um eine einfache systematische Vorgehensweise für den Entwurf, die sicherheitstechnische Bewertung und die Realisierung eines SRECS, das die Anforderungen von IEC 61508 erfüllen soll, zu ermöglichen, verwendet IEC 62061 ein Strukturierungsprinzip, das auf folgenden Architekturelementen beruht (siehe Bild 2/12). (Dieses Strukturierungsprinzip ist auch anwendbar, wenn die sicherheitsrelevanten Teile der Steuerung nach EN 954 realisiert werden sollen.)

Zunächst wird zwischen einer „virtuellen (d.h. funktionalen) Sicht“ und der „realen (d.h. System-) Sicht“ unterschieden. Die funktionale Sicht betrachtet nur die funktionalen Aspekte, unabhängig von der Realisierung durch Hard- und Software. In der virtuellen Sicht wird z.B. nur betrachtet, welche Information zu erfassen ist, wie diese zu verknüpfen ist und welche Aktion daraus resultieren soll. Es wird aber noch keine Aussage darüber gemacht, ob z.B. zum Erfassung der Information redundante Sensoren erforderlich sind oder wie die Aktoren realisiert werden. Erst mit der „realen Sicht“ wird die Realisierung durch das SRECS betrachtet. Hier muss dann entschieden werden, ob z.B. zur Realisierung der Erfassung einer bestimmten Information ein oder zwei Sensoren notwendig sind, um die geforderte Safety Performance zu erreichen. Es werden die folgenden Begriffe definiert.

Begriffe **für die Strukturierung der Funktionen** (funktionale Sicht):

Sicherheitsbezogene Steuerungsfunktion
Steuerungsfunktion mit einem festgelegten Integritätslevel, die von einem SRECS mit dem Ziel, den sicheren Zustand der Maschine aufrecht zu erhalten oder gefährliche Situationen an der Maschine zu verhindern, ausgeführt wird.

Funktionsblock
Kleinste Einheit einer sicherheitsbezogenen Steuerungsfunktion (SRCF), deren Ausfall zum Ausfall der sicherheitsbezogenen Steuerungsfunktion führt.

Anmerkung: In IEC 62061 wird eine SRCF (F) als logische “und“ Verknüpfung der Funktionsblöcke (FB) betrachtet, z.B. F = FB1 & FB2 & ... & FBn.

Die Definition eines Funktionsblockes unterscheidet sich von den in IEC 61131 und anderen Normen verwendeten.

Funktionsblock-Element
Teil eines Funktionsblockes.

Begriffe **für die Strukturierung des realen Systems** (Systemsicht):

Sicherheitsbezogenes elektrisches Steuerungssystem
Elektrisches Steuerungssystem einer Maschine, dessen Ausfall zu einer unmittelbaren Erhöhung des Risikos führen kann.

Anmerkung: Ein SRECS umfasst alle Teile eines elektrischen Steuerungssystems, deren Ausfall zu einer Reduzierung oder dem Verlust der funktionalen Sicherheit führen kann. Dies kann beides, Energie- und Steuerkreise, umfassen.

Teilsystem
Element des Architekturdesigns des SRECS auf oberster Ebene, wobei ein Ausfall irgendeines Teilsystems zu einem Ausfall der sicherheitsbezogenen Steuerungsfunktion führt.

Anmerkung: Im Unterschied zum allgemeinen Sprachgebrauch, in dem „Teilsys-tem" irgendeine unterteilte Einheit bedeuten kann, wird der Begriff „Teilsystem" in IEC 62061 in einer streng definierten Hierarchie der Terminologie verwendet. „Teilsystem" bedeutet die Unterteilung auf oberster Ebene. Die Teile, die aus einer weiteren Unterteilung eines Teilsystems hervorgehen, werden „Teilsystemelemente" genannt.

Teilsystem-Element
Teil eines Teilsystems, das eine einzelne Komponente oder eine Gruppe von Komponenten umfasst.

Mit diesen Strukturierungselementen können Steuerungsfunktionen nach einem eindeutigen Verfahren so strukturiert werden, dass definierte Teile der Funktion (Funktionsblöcke) bestimmten Hardwarekomponenten, den Subsystemen, zugeordnet werden können. Für die einzelnen Subsysteme ergeben sich dadurch klar definierte Anforderungen, sodass sie unabhängig voneinander entworfen und realisiert werden können.

Die Architektur zur Realisierung des vollständigen Steuerungssystems ergibt sich, indem die Subsysteme untereinander so angeordnet werden wie die Funktionsblöcke innerhalb der Funktion (logisch) angeordnet sind.

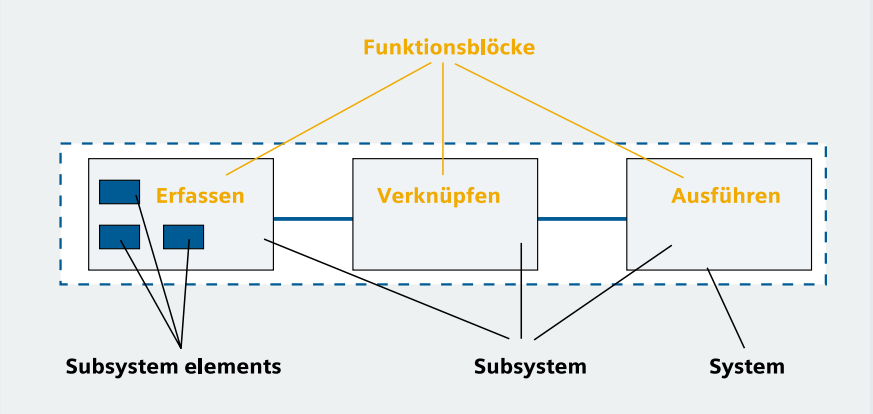


Bild 2/12
Strukturierungselemente der Systemarchitektur

Entwurfsprozess eines sicherheitsrelevanten Steuerungssystems SRECS

Wenn die Spezifikation der Sicherheitsanforderungen vorliegt, kann das vorgesehene Steuerungssystem entworfen und implementiert werden. Ein Steuerungssystem, das den spezifischen Anforderungen einer bestimmten Anwendung genügt, kann im allgemeinen nicht fertig gekauft werden, sondern muss aus verfügbaren Geräten individuell für die betreffende Maschine entworfen und aufgebaut werden.

Im Entwurfsprozess (siehe Bild 2/13) wird schrittweise zunächst für jede Sicherheitsfunktion eine geeignete Architektur des Steuerungssystems entworfen. Anschließend können die Architekturen aller Sicherheitsfunktionen der betreffenden Maschine zu einem Steuerungssystem integriert werden.

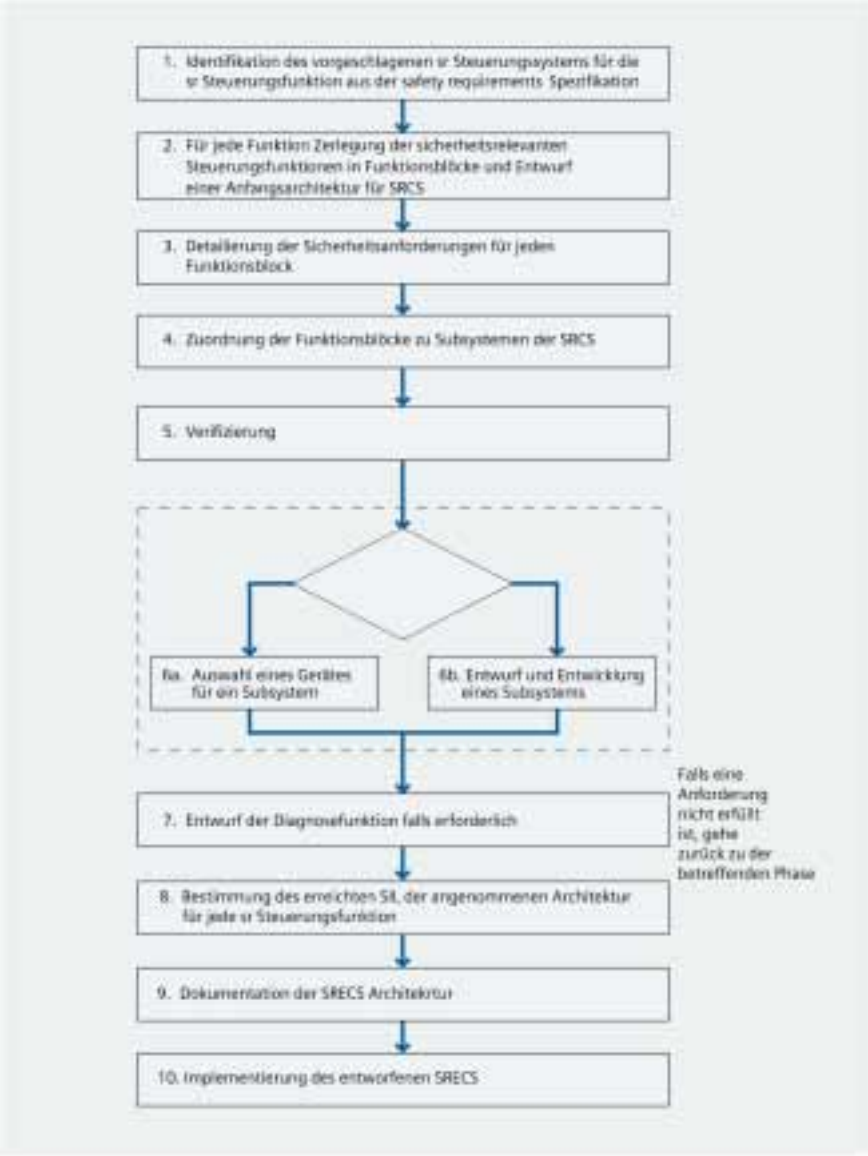

1. Identifikation des vorgeschlagenen sr Steuerungssystems für die sr Steuerungsfunktion aus der safety requirements Spezifikation
2. Für jede Funktion Zerlegung der sicherheitsrelevanten Steuerungsfunktionen in Funktionsblöcke und Entwurf einer Anfangsarchitektur für SRCS
3. Detaillierung der Sicherheitsanforderungen für jeden Funktionsblock
4. Zuordnung der Funktionsblöcke zu Subsystemen der SRCS
5. Verifizierung
6a. Auswahl eines Gerätes für ein Subsystem
6b. Entwurf und Entwicklung eines Subsystems
7. Entwurf der Diagnosefunktion falls erforderlich
Falls eine Anforderung nicht erfüllt ist, gehe zurück zu der betreffenden Phase
8. Bestimmung des erreichten SIL der angenommenen Architektur für jede sr Steuerungsfunktion
9. Dokumentation der SRECS Architektur
10. Implementierung des entworfenen SRECS

Bild 2/13
Designprozess eines sicherheitsrelevanten Steuerungssystems

Strukturierung der Sicherheitsfunktion

Das Grundprinzip des strukturierten Entwurfs besteht darin, jede Steuerungsfunktion in (gedachte) Funktionsblöcke so zu unterteilen, dass diese bestimmten Subsystemen zugeordnet werden können (Bild 2/14). Die Abgrenzung der einzelnen Funktionsblöcke wird dabei so gewählt, dass sie vollständig von bestimmten Subsystemen ausgeführt werden können. Wichtig ist dabei, dass jeder Funktionsblock eine logische Einheit darstellt, die korrekt ausgeführt werden muss damit die gesamte Sicherheitsfunktion korrekt ausgeführt wird.

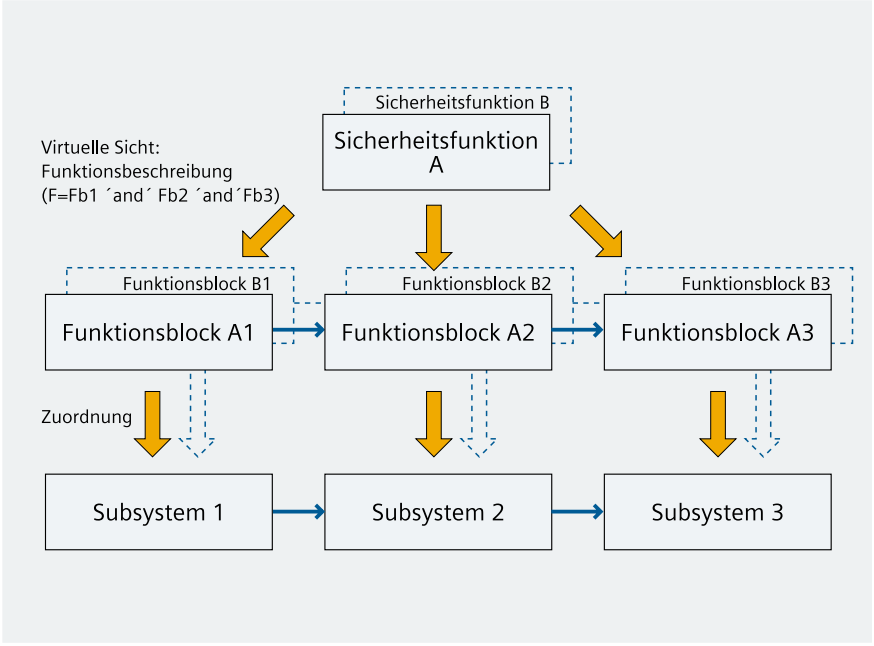


Bild 2/14
Aufteilung einer Sicherheitsfunktion in Funktionsblöcke und Zuordnung zu Subsystemen

Eine Steuerungsfunktion besteht im allgemeinen aus den Grundelementen (Bild 2/15).

- Erfassen (z.B. Maschinenzustände, Bedienkommandos, Zustände von Schutzeinrichtungen)
- Verknüpfen (d.h. Verknüpfen der Zustandsinformationen, Bedienkommandos etc und ggf. eine Aktion ableiten)
- Ausführen (... der von der Verknüpfung initiierten Aktion)

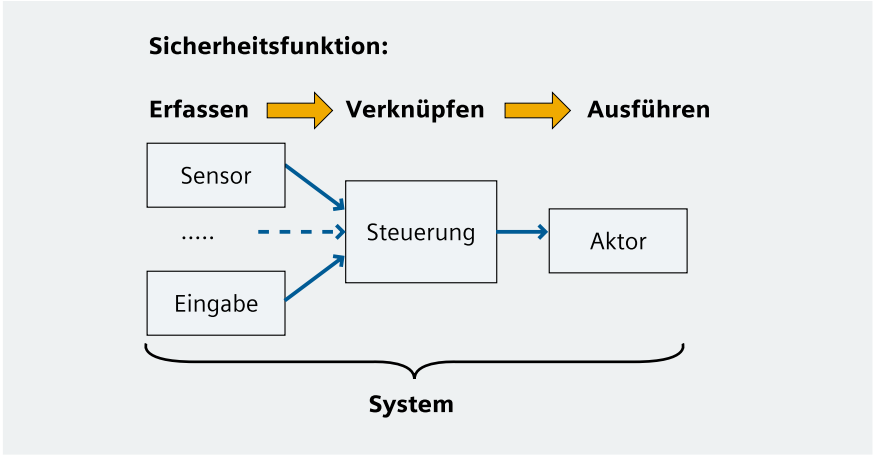


Bild 2/15
Grundelemente einer Steuerungsfunktion

In Sinne der Spezifikation einer Sicherheitsfunktion wird jede zu erfassende Information einem eigenen „Funktionsblock" zugeordnet. Ebenso wird jede auszuführende Aktion einem eigenen „Funktionsblock" zugeordnet. Die Verknüpfung der erfassten Information, das ist die Logik der Sicherheitsfunktion, wird auch als eigene Teilfunktion betrachtet, d.h. sie wird auch einem „Funktionsblock" zugeordnet. Dieser Funktionsblock „Logik" initiiert abhängig von der erfassten Information, die auszuführenden Aktionen. Zu einer Sicherheitsfunktion können also mehrere Funktionsblöcke sowohl zum Erfassen als auch zum Ausführen gehören.

Unterteilung einer Sicherheitsfunktion in Funktionsblöcke für Beispiel (2) der bei den Maßnahmen zur Risikoreduzierung beschriebenen einfachen Sicherheitsfunktion F, die den Zugang zum Gefahrenbereich bei laufender Maschine verhindert :

F = Während des Produktionsbetriebes alle Zugänge zum Arbeitsbereich der Maschine (Fertigungszelle) verriegeln.

Die Unterteilung ergibt die Funktionsblöcke:
F1 = Erfassen der eingestellten
F2 = Logik: Abhängig vom eingestellten Betriebsmodus Verriegelung der Türen A und B veranlassen,
F3 = Verriegelung Tür A ausführen
F4 = Verriegelung Tür B ausführen
Dabei sind die einzelnen Funktionsblöcke so abgegrenzt, dass zur korrekten Ausführung der Sicherheitsfunktion F alle ihre Funktionsblöcke korrekt ausgeführt werden müssen. Es gilt also die logische Verknüpfung

F = F1 `und´ F2 `und´ F3 `und´ F4;

Verhalten im Fehlerfall:
Falls ein Fehler z.B. in einer Verriegelung festgestellt wird, so dass ein unerlaubter Zugang zur Maschine nicht mehr ausgeschlossen werden kann, muss die Maschine angehalten werden.

Aufgrund dieser Zusammenhänge kann die für die gesamte Sicherheitsfunktion geforderte Safety Performance folgendermaßen auf die Funktionsblöcke und die ihnen zugeordneten Subsysteme übertragen werden. (Wegen ihrer unterschiedlichen Konzepte werden EN 954 und IEC 62061 im Folgenden getrennt betrachtet.)

Hinweis:

In diesem ersten Schritt werden nur die Abgrenzung der Funktionsblöcke und die Unterteilung des Systems in Subsysteme (wie oben definiert!) vorgenommen. Eine evtl. notwendige Betrachtung der Subsysteme selber erfolgt erst im nächsten Schritt, der weiter unten beschrieben wird.

Erforderliche Safety Performance der Subsysteme

Die Safety Performance eines sicherheitsrelevanten Steuerungssystems bezieht sich immer auf eine vollständige Sicherheitsfunktion, so wie in der Safety Requirements Spezifikation (für das System) festgelegt. Mit dem oben beschriebenen Strukturierungsprinzip kann daraus die geforderte Safety Performance für die einzelnen Subsysteme abgeleitet werden.

Wegen der Unterschiede in der Systematik der Anforderungen von IEC 61508 bzw. IEC 62061 einerseits und EN 954 (bzw. ISO 13849) andererseits gibt es auch Unterschiede in der Bestimmung der Details der erforderlichen Safety Performance des Subsystems.

Safety Performance eines Subsystems nach IEC 61508 bzw. IEC 62061

Die „Safety Integrity" nach IEC 61508 (und somit auch IEC 62061) erfordert die Erfüllung der drei Grundanforderungen:
(1) systematische Integrität),
(2) strukturelle Einschränkungen, d.h. Fehlertoleranz und
(3) begrenzte Wahrscheinlichkeit gefährlicher zufälliger (Hardware) Ausfälle (PFH_D).
die entsprechend dem SIL abgestuft sind.

Die für die ganze Funktion geforderte systematische Integrität (1) des Systems sowie die strukturellen Einschränkungen (2) gelten für die einzelnen Subsysteme genauso wie für das System. D.h. wenn jedes einzelne Subsystem die geforderte systematische Integrität und die strukturellen Einschränkungen eines bestimmten SIL erfüllt, dann erfüllt sie das System auch. Erfüllt jedoch ein Subsystem nur die geringeren Anforderungen eines niedrigeren SIL, dann begrenzt das den SIL, den das System erreichen kann. Man spricht deshalb vom „SIL claim limit" (SIL CL) eines Subsystems.

- systematische Integrität:
  SIL SYS <= SIL CL_{lowest}
- strukturelle Einschränkungen:
  SIL SYS <= SIL CL_{lowest}

Für die Verbindung der Subsysteme untereinander müssen die gleichen Anforderungen erfüllt werden. Dazu werden Einzelverdrahtungen als Bestandteil jeweils eines der beiden verbundenen Subsysteme betrachtet. Bei Busverbindung sind Sende- und Empfangshardware und –software Bestandteile der Subsysteme.

Die Begrenzung der Wahrscheinlichkeit gefahrbringender zufälliger Fehler (3) gilt für die gesamte Funktion, d.h. sie darf von allen Subsystemen zusammen nicht überschritten werden. Es gilt somit:

$$PFH_D = PFH_{D1} + \ldots + PFH_{Dn}$$

Bei Busverbindungen muss zusätzlich noch die Wahrscheinlichkeit möglicher Datenübertragungsfehler (P_{TE}) addiert werden.

Die hier erwähnten Parameter SIL CL, PFH_{Dn} und P_{TE} können von den Herstellern der Subsysteme in den zugehörigen Datenblättern angeben werden.

Sicherheitsparameter von Subsystemen

Die Beschreibung eines Subsystems umfasst neben der genauen Spezifikation seiner Funktionalität und Einsatzbedingungen auch die Sicherheitsparameter zur Angabe seiner Safety Performance.

Für Design nach IEC 62061

- den maximalen SIL, für den es geeignet ist, SIL CL
- die Wahrscheinlichkeit (gefährlicher) zufälliger Fehler, PFH_D
- und bei Busanschluss die Wahrscheinlichkeit unerkannter Datenübertragungsfehler, P_{TE}

Systemdesign für eine Sicherheitsfunktion

Architekturentwurf

Die Architektur eines Steuerungssystems für eine bestimmte Sicherheitsfunktion entspricht in ihrer logischen Struktur der zuvor ermittelten Struktur der Sicherheitsfunktion. Zur Festlegung der realen Systemstruktur werden die Funktionsblöcke der Sicherheitsfunktion bestimmten Subsystemen zugeordnet. Die Subsysteme werden dann so miteinander verschaltet, dass die durch die Funktionsstruktur vorgegebenen Verbindungen hergestellt werden. Die physikalische Verschaltung erfolgt entsprechend den Eigenschaften der gewählten Technik, z.B. durch Einzelverdrahtung (Punkt zu Punkt) oder durch Busverbindung.

Für weitere Sicherheitsfunktionen der Maschine oder Anlage wird ebenso verfahren. Dabei können aber Funktionsblöcke, die denjenigen anderer Sicherheitsfunktionen entsprechen, denselben Subsystemen zugeordnet werden. Wenn also z.B. für zwei verschiedene Funktionen die selbe Information erfasst werden muss (z.B. Position derselben Schutztür), dann können dazu dieselben Sensoren verwendet werden.

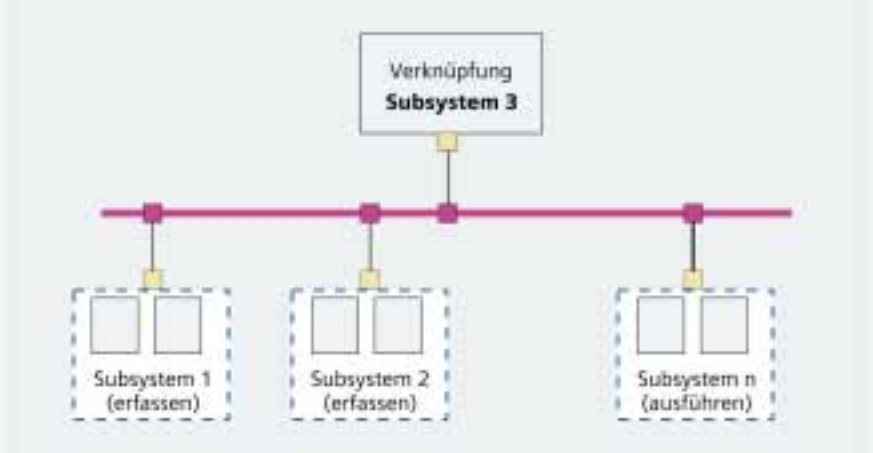


Bild 2/16
Beispiel einer Systemarchitektur für eine Sicherheitsfunktion

Auswahl geeigneter Geräte (Subsysteme)

Ein Subsystem, das zur Implementierung einer Sicherheitsfunktion eingesetzt werden soll, muss die geforderte Funktionalität haben und den betreffenden Anforderungen von IEC 62061 genügen. Mikroprozessorbasierte Subsysteme müssen IEC 61508 für den entsprechenden SIL erfüllen.
Es können auch Geräte, die eine bestimmte Kategorie nach EN 954 erfüllen, als Subsysteme eingesetzt werden. Die notwendigen Anforderungen zur Integration dieser Geräte in das Designkonzept von IEC 62061 sind im Abschnitt „Realisierung von Subsystemen“ beschrieben.

Für Design nach IEC 62061

Die einzelnen Subsysteme müssen die in der Spezifikation geforderten Sicherheitsparameter (SIL CL und PFH_D) erfüllen.

Es können auch Subsysteme eingesetzt werden, die bestimmte Kategorien erfüllen. Auf Basis der angegebenen Kategorie können die entsprechenden Sicherheitsparameter „SIL CL“ und „PFH_D“ bestimmt werden (siehe IEC 62061 Abschnitte 6.7.6 und 6.7.8).

In vielen Fällen benötigen Geräte noch zusätzliche Fehleraufdeckungsmaßnahmen (Diagnose), um die für ihre Verwendung als Subsystem angegebene Safety Performance tatsächlich zu erreichen. Diese Fehleraufdeckung kann z.B. durch Zusatzgeräte (z.B. 3TK28) oder entsprechende Software-Diagnosebausteine in der Logikverarbeitung erfolgen (siehe „Subsystemdesign“). Für diesen Fall muss die Beschreibung des Gerätes entsprechende Informationen enthalten.

Wenn kein geeignetes Gerät zur Verfügung steht, das den Anforderungen eines so spezifizierten Subsystems genügt, muss es aus verfügbaren Geräten zusammengesetzt werden. Das erfordert einen nächsten Entwurfsschritt. Siehe dazu Abschnitt „Subsystem Design“.

Realisierung des sicherheitsrelevanten Steuerungssystems

Ein sicherheitsrelevantes Steuerungssystem muss so realisiert werden, dass es alle Anforderungen entsprechend dem verlangten SIL erfüllt. Ziel ist es, die Wahrscheinlichkeit sowohl systematischer als auch zufälliger Fehler, die zu gefährlichem Versagen der Sicherheitsfunktion führen können, ausreichend klein zu machen. Folgende Aspekte sind zu beachten

- Hardwareintegrität, d.h. Architektureinschränkungen, (Fehlertoleranz) und begrenzte Versagenswahrscheinlichkeit,
- Systematische Integrität, d.h. Anforderungen zur Vermeidung und Beherrschung von Fehlern,
- Verhalten bei Aufdecken eines Fehlers und Softwaredesign/ -entwicklung

Hardwareintegrität

Jedes Subsystem muss eine für den SIL des Systems ausreichende Fehlertoleranz haben. Diese ist abhängig davon, wie groß der Anteil der Fehler, die in eine sichere Richtung gehen, bezogen auf die Wahrscheinlichkeit aller möglichen Fehler des Subsystems ist. Potentiell gefährliche Fehler eines Subsystems, die durch Diagnose rechtzeitig aufgedeckt werden, gehören dabei zu den Fehlern, die in eine sichere Richtung gehen.

Die erlaubte Wahrscheinlichkeit des Versagens einer Sicherheitsfunktion ist durch den in der Spezifikation festgelegten SIL begrenzt (siehe Bild 2/17).

Systematische Integrität

Es sind Maßnahmen sowohl zur Vermeidung systematischer Fehler als auch zur Beherrschung im System verbliebener Fehler anzuwenden:

Vermeidung systematischer Fehler

- Das System ist gemäß Sicherheitsplan zu installieren
- Die Herstellerangaben der verwendeten Geräte sind zu befolgen
- Die elektrische Installation gemäß IEC 60204-1 (7.2, 9.1.1 und 9.4.3) auszuführen
- Das Design auf seine Eignung und Korrektheit überprüfen
- Verwendung eines rechnergestütztes Tools, das auf vorkonfigurierte und erprobte Elemente benutzt.

Beherrschung systematischer Fehler

- Verwendung des Prinzips der Energieabschaltung
- Maßnahmen zur Beherrschung temporärer Subsystemausfälle oder -störungen, z.B. wegen Spannungsunterbrechungen
- bei Verbindung der Subsysteme durch einen Bus sind die Anforderungen von IEC 61508-2 an die Datenkommunikation zu erfüllen (z.B. PROFIsafe und ASIsafe)
- Fehler in der Verbindung (Verdrahtung) und den Schnittstellen der Subsysteme müssen erkannt und geeignete Reaktionen veranlasst werden. Für die systematische Behandlung werden die Schnittstellen und die Verdrahtung als Bestandteil des betreffenden Subsystems betrachtet.

Details siehe IEC 62061 6.4

Verhalten bei Aufdecken eines Fehlers

Wenn Fehler eines Subsystems zu einem gefährlichen Versagen einer Sicherheitsfunktion führen können, müssen diese rechtzeitig aufgedeckt und eine geeignete Reaktion veranlasst werden, um eine Gefahr zu vermeiden. In welchem Maße automatische Fehleraufdeckung (Diagnose) notwendig ist, hängt von den Ausfallraten der verwendeten Geräte und dem zu erreichenden SIL des Systems (bzw. der geforderten PFH des Subsystems) ab.

Wie sich das System bzw. Subsystem bei Erkennen eines Fehlers verhalten muss, ist abhängig von der Fehlertoleranz des betreffenden Subsystems. Führt der erkannte Fehler nicht direkt zum Versagen der Sicherheitsfunktion, d.h. Fehlertoleranz > 0, ist eine Fehlerreaktion nicht sofort notwendig, sondern erst wenn die Wahrscheinlichkeit für das Auftreten eines zweiten Fehlers zu groß wird (in der Regel sind das Stunden oder Tage). Führt der erkannte Fehler direkt zum Versagen der Sicherheitsfunktion, d.h. Fehlertoleranz = 0, ist eine Fehlerreaktion sofort, d.h. bevor eine Gefahr eintritt, notwendig.

Erreichte Safety Performance

Für jede Sicherheitsfunktion ist in ihrer Spezifikation festgelegt, welche Safety Performance sie benötigt. Diese muss von dem sicherheitsrelevanten Steuerungssystem erfüllt werden.

Welche Safety Performance ein System erreicht, muss für jede Sicherheitsfunktion ermittelt werden. Dies erfolgt anhand der Architektur des Systems und der Sicherheitsparameter der Subsysteme, die an der Ausführung der betrachteten Sicherheitsfunktion beteiligt sind.

Design nach IEC 62061

Der erreichte SIL wird begrenzt durch die „SIL-Eignung" seiner Subsysteme. Der niedrigste Wert der eingesetzten Subsysteme begrenzt den SIL des Systems auf diesen Wert (Das schwächste Glied einer Kette bestimmt deren Festigkeit.).

systematische Integrität:
SIL SYS <= SIL CL_{lowest}

strukturelle Einschränkungen:
SIL SYS <= SIL CL_{lowest}

Für die Verbindung der Subsysteme untereinander müssen die gleichen Anforderungen erfüllt werden. Dazu werden Einzelverdrahtungen als Bestandteil jeweils eines der beiden verbundenen Subsysteme betrachtet. Bei Busverbindung sind Sende- und Empfangshardware und -software Bestandteile der Subsysteme.

Außer dieser prinzipiellen Eignung muss außerdem die Wahrscheinlichkeit gefährlichen Versagens jeder Sicherheitsfunktion betrachtet werden. Dieser Wert ergibt sich durch einfache Addition der Versagenswahrscheinlichkeiten der an der Funktion beteiligten Subsysteme:

$PFH_D = PFH_{D1} + ... + PFH_{Dn}$

Bei Busverbindungen muss zusätzlich noch die Wahrscheinlichkeit möglicher Datenübertragungsfehler (PTE) addiert werden.

Der für eine bestimmte Sicherheitsfunktion so ermittelte Wert muss kleiner (oder gleich) sein als der durch den zugehörigen SIL festgelegte Wert.

Design nach EN 954

Die erreichte Kategorie des Systems entspricht der Kategorie seiner Subsysteme.

Werden rechnerbasierte Subsysteme und Buskommunikation eingesetzt, so müssen diese bestimmte SIL nach 61508 erfüllen. Dabei gilt folgende Zuordnung: Ein für SIL 1 geeignetes Subsystem kann für Kategorie 2 eingesetzt werden und entsprechend SIL 2 für Kategorie 3 oder SIL 3 für Kategorie 4.

Wahrscheinlichkeit eines gefahrbringenden Fehlers pro Stunde (PFH_D)			
	SIL 1	SIL 2	SIL 3
PFH_D	$< 10^{-5}$	$< 10^{-6}$	$< 10^{-7}$

Bild 2/17
Grenzwerte der Wahrscheinlichkeiten gefahrbringender Fehler einer Sicherheitsfunktion

Systemintegration für alle Sicherheitsfunktionen

Nachdem die Architekturen für alle Sicherheitsfunktionen entworfen sind, folgt als nächster Schritt die Integration dieser funktionsspezifischen Architekturen zu dem vollständigen sicherheitsrelevanten Steuerungssystem.

Dort, wo mehrere Sicherheitsfunktionen identische Funktionsblöcke haben, können für deren Realisierung gemeinsame Subsysteme verwendet werden. Beispielsweise braucht man nur eine Sicherheits-SPS zur Implementierung der Logik aller Sicherheitsfunktionen. Oder wenn zur Beseitigung unterschiedlicher Gefährdungen (d.h. unterschiedliche Sicherheitsfunktionen) der Zustand derselben Schutztür erfasst werden muss, braucht der notwendige Sensor an dieser Tür nur einmal installiert zu werden.

Auf die Safety Integrity, die für die einzelnen Funktionen bereits bestimmt wurde, hat dies keinen Einfluss. Lediglich bei den elektromechanischen (verschleißbehafteten) Geräten muss das bei der Bestimmung ihrer Schalthäufigkeit berücksichtigt werden.

Entwurf und Realisierung von Subsystemen

Als Alternative zur Auswahl eines vorhandenen Subsystems kann ein Subsystem auch aus Geräten, die alleine nicht die Sicherheitsanforderungen erfüllen, so zusammengesetzt werden, dass das Subsystem dann die notwendige Safety Performance erreicht. Das ist bezüglich der systematischen Integrität und der strukturellen Einschränkungen das durch den SIL der Sicherheitsfunktion vorgegebene SIL claim limit (SIL CL). Für die Wahrscheinlichkeit gefahrbringender zufälliger Fehler (PFH_D) wurden beim Entwurf der Systemarchitektur die maximalen PFH Werte für die einzelnen Subsysteme festgelegt.

> IEC 62061: The safety performance of a subsystem is characterized by the SILCL determined by its architectural constraints (6.7.6), its SILCL due to systematic integrity (6.7.9) and its probability of dangerous random hardware failure (6.7.8).

Zumindest für SIL 2 und SIL 3 wird im allgemeinen Redundanz benötigt. Sei es, um die notwendige Fehlertoleranz zu erreichen, oder um Fehleraufdeckung (Diagnose) zu ermöglichen. Die Kombination zweier Geräte zu einem Subsystem kann aber auch erforderlich sein, um die Wahrscheinlichkeit eines gefährlichen Versagens zu verringern.

> Wenn z.B. für die Zugangsverriegelungen des Beispiels (2) der Risikoreduzierungsmaßnahmen SIL 2 oder 3 (bzw. Kategorie 3 oder 4) gefordert ist, reichen einfache Türverriegelungen oder Endschalter nicht aus. Es müssen zur Verriegelung jeder Tür z.B. zwei Zuhaltungen eingesetzt und Maßnahmen zur Fehleraufdeckung implementiert werden.

Die genauen Anforderungen für Entwurf und Realisierung von Subsystemen sind in IEC 62061 Abschnitt 6.7 und 6.8 beschrieben. Die folgende Beschreibung vermittelt einen Überblick.

Subsystem Architekturentwurf

Eine spezielle Subsystemarchitektur ist immer dann zu entwerfen, wenn mit den für eine bestimmte Aufgabe (Teilfunktion, „Funktionsblock") vorgesehenen Geräten die notwendige Safety Integrity (Safety Performance) nicht direkt erreicht wird. Im Allgemeinen können die sicherheitstechnischen Eigenschaften

- Geringe Versagenswahrscheinlichkeit
- Fehlertoleranz, Fehlerbeherrschung
- Fehleraufdeckung

nur durch besondere Architekturmaßnahmen erreicht werden. In welchem Umfang bestimmte Maßnahmen notwendig sind, ist abhängig von der geforderten Safety Performance (Safety Integrity).

Dem Subsystem ist eine bestimmte (Teil-)Funktion, der Funktionsblock, zugeordnet (z.B. Zuhalten einer Tür). Dieser Funktionsblock wird zunächst (gedanklich) in einzelne Elemente (Funktionsblockelemente) unterteilt, die dann bestimmten Geräten, den Subsystemelementen, zugeordnet werden können (siehe Bild 2/18). Im Allgemeinen kann die gleiche Funktion zwei Funktionsblockelementen zugeteilt werden (die Funktion wurde praktisch verdoppelt). Wenn diese Funktionsblockelemente dann durch jeweils eigene Geräte realisiert werden, hat das Subsystem eine einfache Fehlertoleranz (einfache Redundanz).

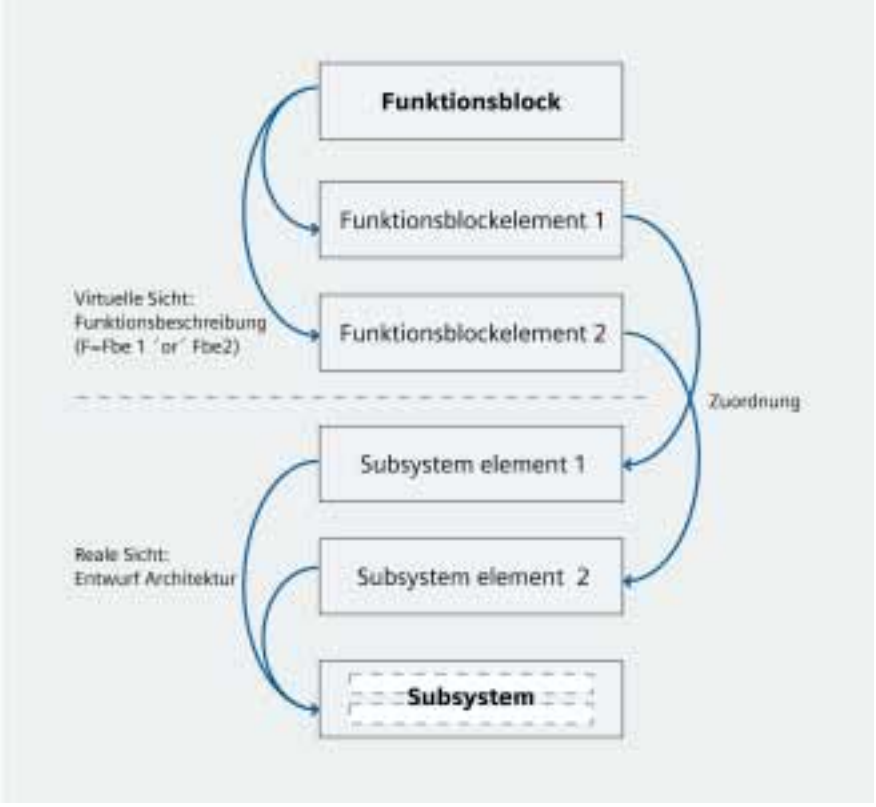


Bild 2/18
Beispiel für den Entwurf einer Subsystemarchitektur

Reicht zur Realisierung von Funktionsblock F3 „Verriegelung Tür A ausführen" des Beispiels (2) eine einfache Zuhaltung nicht aus, um die spezifizierte Safety Performance zu erreichen, kann mit den beiden folgenden Lösungsansätzen ein Subsystem mit höherer Safety Performance realisiert werden.

a) Parallelschalten einer zweiten Türzuhaltung → einfache Redundanz.
b) Ergänzen der Türzuhaltung durch eine Türpositionsüberwachung → Fehleraufdeckung

Im Beispiel a) für homogene Redundanz ist der Funktionsblock „Verriegelung Tür A ausführen" auf zwei gleiche Funktionsblockelemente aufgeteilt, von denen jede diese Funktion hat. Zur Aufdeckung möglicher Fehler sind trotz redundanter Anordnung weitere Maßnahmen notwendig.
Im Beispiel b) wird der Funktionsblock „Verriegelung Tür A ausführen" nicht weiter aufgeteilt. Er ist eins zu eins einem Funktionsblockelement zugeordnet. Die zusätzliche Türpositionsüberwachung dient der Fehlererkennung. Sie verbessert nicht die Türzuhaltung selber. Aber mit der Überwachung kann erkannt werden, wenn die Türzuhaltung versagt, und es kann eine entsprechende Reaktion veranlasst werden.

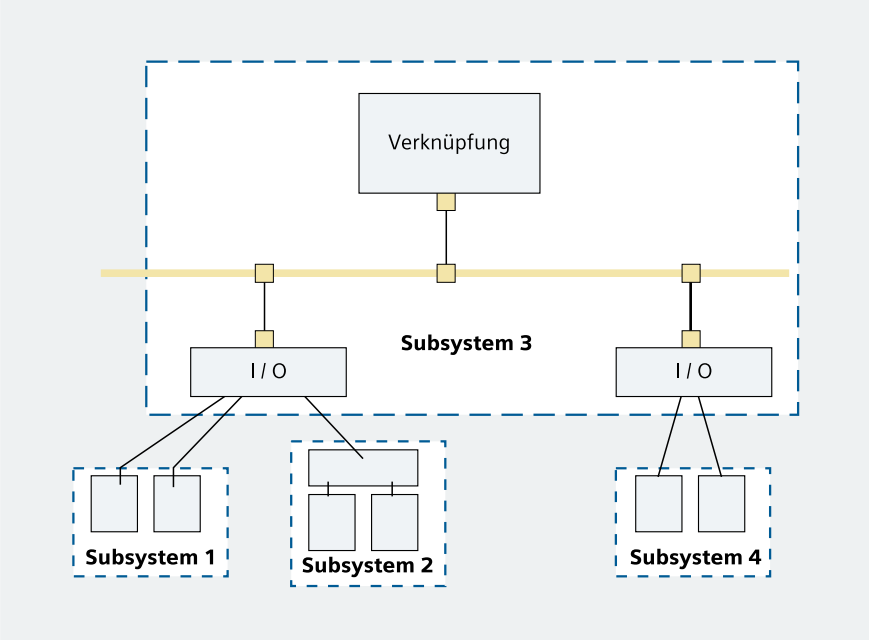


Bild 2/19
Beispiele für Subsystemarchitekturen

Fehleraufdeckung eines Subsystems (Diagnose)

Bei einem Subsystem ohne Fehlertoleranz führt jeder Fehler zum Verlust der Funktion. Das Versagen der Funktion kann, abhängig von der Art des Fehlers, zu einem gefährlichen oder sicheren Zustand der Maschine führen. Kritisch sind die Fehler, die einen gefährlichen Zustand der Maschine zur Folge haben. Sie werden als „gefahrbringende Fehler" bezeichnet. Um zu vermeiden, dass ein gefahrbringender Fehler tatsächlich zu einer Gefährdung führt, kann man bestimmte Fehler durch Diagnose aufdecken und die Maschine in einen sicheren Zustand bringen, bevor die Gefährdung entsteht. Ein durch die Diagnose aufgedeckter gefahrbringender Fehler kann so in einen „sicheren Fehler" umgewandelt werden.

Bei einem redundanten Subsystem führt der erste Fehler noch nicht zum Versagen seiner Funktion. Erst ein weiterer Fehler kann den Verlust der Funktion verursachen. Um das Versagen des Subsystems zu vermeiden, muss also der erste Fehler aufgedeckt werden bevor ein zweiter Fehler auftritt. Die Fehleraufdeckung muss natürlich mit einer geeigneten Systemreaktion verbunden sein. Im einfachsten Fall wird z.B. die Maschine angehalten, um sie in einen sicheren Zustand zu bringen, der die (fehlerhafte) Sicherheitsfunktion nicht benötigt.

Durch die Fehleraufdeckung (Diagnose) verbunden mit einer geeigneten Fehlerreaktion wird in beiden Fällen die Wahrscheinlichkeit eines gefährlichen Versagens der betreffenden Sicherheitsfunktion verringert. In welchem Maße die Wahrscheinlichkeit verringert wird hängt u.a. davon ab, wie viele der möglichen gefährlichen Fehler erkannt werden. Das Maß dafür ist der Diagnosedeckungsgrad (diagnostic coverage DC).

Die Fehleraufdeckung eines Subsystems kann im betreffenden Subsystem selber oder durch ein anderes Gerät, z.B. die Sicherheits-SPS erfolgen. Bild 2/20 zeigt Beispiele für die unterschiedliche Anordnung der Diagnose.

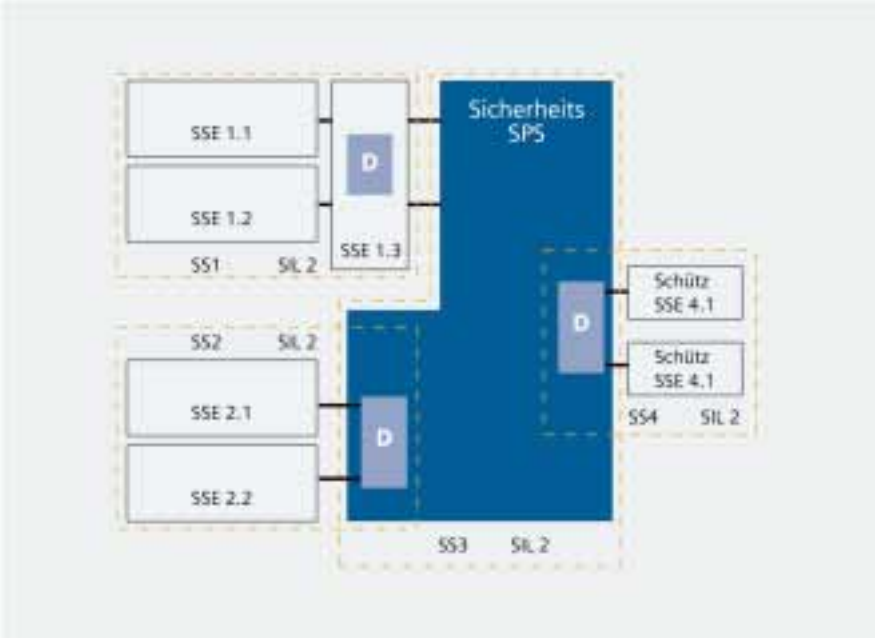


Bild 2/20
Anordnung der Diagnosefunktionen von Subsystemen

Systematische Integrität eines Subsystems

Bei Design und Implementierung eines Subsystems müssen Maßnahmen sowohl zur Vermeidung als auch zur Beherrschung systematischer Fehler getroffen werden, z.B.:

- Die eingesetzten Geräte müssen die entsprechenden internationalen Normen erfüllen.
- Die vom Hersteller angegebenen Anwendungsbedingungen müssen eingehalten werden.
- Das Design und die verwendeten Materialien müssen so sein, dass sie allen zu erwartenden Umgebungsbedingungen standhalten.
- Das Verhalten aufgrund von Umgebungseinflüssen muss vorherbestimmt sein, sodass ein sicherer Zustand der Maschine erhalten werden kann.
- Online Fehleraufdeckung
- Zwangsbetätigung zur Initiierung einer Schutzmaßnahme.

Die in IEC 62061 beschriebenen Anforderungen betreffen nur das Design elektrischer Subsysteme geringer Komplexität, also keine Subsysteme mit Mikroprozessoren. Die geforderten Maßnahmen gelten für alle SIL gleichermaßen.

Ausfallwahrscheinlichkeit (PFH_D) eines Subsystems

Die möglichen Ausfälle werden unterschieden in „sichere" oder „gefahrbringende" Ausfälle. Dabei sind die gefahrbringenden Ausfälle eines Subsystems wie folgt definiert.

Gefahrbringender Ausfall

Ausfall eines SRECS, eines Subsystems oder Subsystemelementes mit dem Potenzial, eine Gefährdung oder funktionsfähigen Zustand zu verursachen. Anmerkung: Ob ein solcher Zustand eintritt oder nicht, kann von der Systemarchitektur abhängen; in Systemen mit mehrfachen Kanälen zur Verbesserung der Sicherheit führt ein gefahrbringender Hardwareausfall mit geringerer Wahrscheinlichkeit zum gefahrbringenden Gesamtzustand oder zu einem Funktionsausfall.

Das bedeutet z.B.: Bei einem redundanten Subsystem (d.h. Fehlertoleranz 1) wird ein Fehler eines Kanals als gefahrbringend bezeichnet, wenn er potenziell gefahrbringend ist, d.h. bei nicht vorhandenem zweiten Kanal zu einem gefährlichen Zustand der Maschine führen kann.

Für die Sicherheitsanforderungen ist nur die Wahrscheinlichkeit gefahrbringender Ausfälle maßgebend. Die so genannten „sicheren Fehler" verschlechtern zwar die Verfügbarkeit des Systems, verursachen aber keine Gefährdung.

Die Ausfallwahrscheinlichkeit eines Subsystems ist abhängig von den Ausfallraten der Geräte aus denen das Subsystem aufgebaut ist, der Architektur und den Diagnosemaßnahmen. Für die beiden gebräuchlichsten Architekturen sind die Formeln im Folgenden beschrieben. Sie gelten unter bestimmten Voraussetzungen, die in IEC 62061 präzisiert sind:

Bei ausreichend kleinen ($1 >> \lambda . T$) Fehlerraten (λ) der Subsystemelemente kann die folgende Gleichung angewendet werden:

$\lambda = 1/MTTF$

Für elektromechanische Geräte ist die Ausfallrate (λ) zu bestimmen, in dem der B10-Wert des Gerätes und die Schaltspielrate C der spezifizierten Anwendung in folgende Gleichung eingesetzt wird:

$\lambda = 0.1 * C/B_{10}$

In den Formeln werden folgende Begriffe verwendet:

$\lambda = \lambda_S + \lambda_D$;
wobei λ_S die Rate ungefährlicher Ausfälle und λ_D die Rate gefahrbringender Ausfälle ist.

$PFH_D = \lambda_D * 1h$;
mittlere Wahrscheinlichkeit gefahrbringender Ausfälle innerhalb einer Stunde

T2 : Diagnose-Testintervall

T1:
Proof-Test-Intervall oder Lebensdauer, jeweils der kleinere Wert

Durch die Diagnose kann meist nur ein gewisser Anteil der Fehler aufgedeckt werden. Wie groß dieser Anteil ist, wird durch den Diagnosedeckungsgrad angegeben.

Der Diagnosedeckungsgrad kann mit folgender Formel berechnet werden:

$DC = \Sigma \lambda_{DD} / \lambda_{Dtotal}$

wobei λ_{DD} die Rate der aufgedeckten gefahrbringenden Hardwareausfälle und λ_{Dtotal} die Rate aller gefahrbringenden Hardwareausfälle ist.

Für die Bestimmung des Diagnosedeckungsgrades werden die einzelnen Fehler (Ausfallmodi) entsprechend ihrer relativen Häufigkeit gewichtet. In Tabelle D.1 von IEC 62061 sind dazu typische Verhältniszahlen für eine Reihe von Geräten angegeben. Bei der Ermittlung des Fehleraufdeckungsgrades für ein Subsystem müssen alle seine Teile (Subsystemelemente) betrachtet werden. Dazu gehören z.B. auch die Klemmen und die Verdrahtung der einzelnen Teile.

Struktur ohne Fehlertoleranz mit Diagnose

Bei dieser Struktur (Bild 2/21) versagt das Subsystem, wenn ein beliebiges seiner Elemente versagt, d.h. ein einzelner Fehler führt zum Versagen der eigentlichen Sicherheitsfunktion. Dies bedeutet aber noch nicht zwingend einen gefährlichen Verlust der Sicherheitsfunktion. Abhängig von der Art des Fehlers kann die Maschine in einen sicheren oder einen gefährlichen Zustand gehen, d.h. das Subsystem hat einen „sicheren" oder einen „gefährlichen" Fehler. Ist die Wahrscheinlichkeit gefährlicher Fehler (PFH_S) größer als in der Spezifikation vorgegeben, müssen diese Fehler durch Diagnose aufgedeckt und eine Fehlerreaktion veranlasst werden bevor eine Gefahr entsteht. Dadurch werden gefährliche Fehler zu sicheren Fehlern und folglich die Wahrscheinlich eines gefährlichen Versagens des Subsystems verringert, sodass evtl. die in der Spezifikation erlaubte Versagenswahrscheinlichkeit erreicht wird.

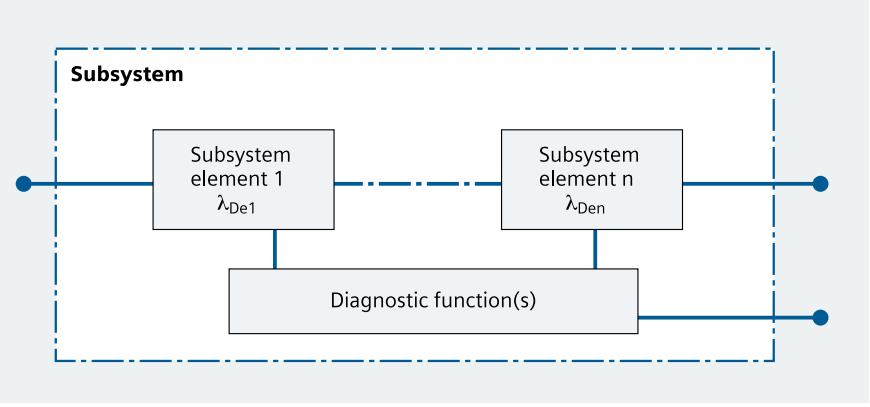


Bild 2/21
Logische Struktur eines Subsystems ohne Fehlertoleranz mit Diagnose

(Hinweis: Bei der in Bild 2/21 dargestellten Struktur hat das Subsystem eine Diagnose mit unabhängigem Abschaltpfad. Mit dieser Struktur kann, abhängig vom Diagnosedeckungsgrad, auch Kategorie 2, 3 oder 4 nach EN 954-1 erfüllt werden.)

IEC 62061 6.7.8.2.4

Jeder unerkannte gefährliche Fehler eines Subsystemelements führt zu einem gefahrbringenden Versagen der sicherheitsrelevanten Steuerungsfunktion. Wenn ein Fehler eines Subsystemelements aufgedeckt wird, initiiert die Diagnosefunktion eine Fehlerreaktionsfunktion. Bei dieser Struktur ist die Wahrscheinlichkeit gefahrbringender Fehler des Subsystems:

$\lambda_{DssC} = \lambda_{De1} (1 - DC1) + ...+ \lambda_{Den}(1 - DCn)$

$PFHDssC = \lambda_{DssC} * 1h$

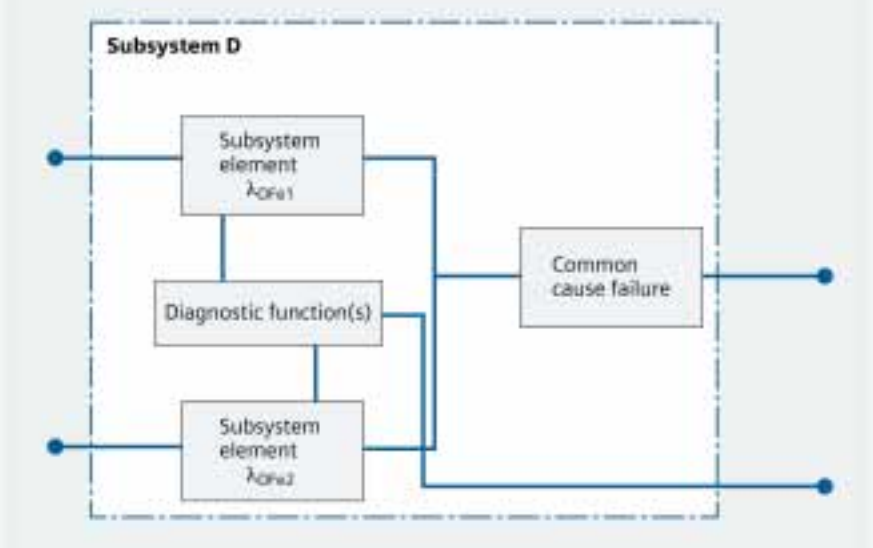


Bild 2/22
Logische Struktur eines Subsystems mit einfacher Fehlertoleranz mit Diagnose

Struktur mit einfacher Fehlertoleranz und mit Diagnose

Bei dieser Struktur (siehe Bild 2/22) führt der erste Fehler noch nicht zum Versagen der Funktion. Der Fehler muss aber aufgedeckt werden, bevor die Wahrscheinlich für das Auftreten eines zweiten Fehlers, d.h. des Versagens des Subsystems, die in der Spezifikation gegebene Grenze überschreitet.

Außer den unabhängigen, zufälligen Fehlern ist bei redundanten Subsystemen noch die Möglichkeit von Fehlern gemeinsamer Ursache (common cause failure) zu beachten. Gegen solche Fehler hilft homogene Redundanz nicht. Beim Entwurf müssen deshalb systematische Maßnahmen getroffen werden, die ihre Wahrscheinlichkeit ausreichend gering machen. Da common cause Fehler nie ganz ausgeschlossen werden können, müssen sie bei der Berechnung der Ausfallwahrscheinlichkeit des Subsystems berücksichtigt werden. Dies erfolgt mit Hilfe des Common Cause Faktors (β), mit dem die Wirksamkeit der getroffenen Maßnahmen bewertet wird. In Annex F von IEC 62061 befindet sich eine Tabelle zur Bestimmung des erreichten Common Cause Faktors.

Bei dieser Struktur führt ein einzelner Ausfall eines beliebigen Subsystemelements nicht zum Ausfall der sicherheitsrelevanten Steuerungsfunktion. Zur Berechnung der Ausfallwahrscheinlichkeit des Subsystems werden die folgenden Formelzeichen verwendet:

T2: Diagnose-Testintervall;

T1: Proof-Testintervall oder Lebensdauer, jeweils der kleinere Wert;

β: β-Faktor, d.h. Empfindlichkeit für common cause Fehler;

$\lambda_D = \lambda_{DD} + \lambda_{DU}$; wobei λ_{DD} die Rate der aufgedeckten und λ_{DU} die Rate der nicht aufgedeckten gefährlichen Fehler ist.

$\lambda_{DD} = \lambda_D * DC$
$\lambda_{DU} = \lambda_D * (1\text{-}DC)$

Bei der Berechnung werden zwei Varianten unterschieden.

Die Subsystemelemente beider Kanäle sind unterschiedlich:

λ_{De1}: Rate gefährlicher Fehler von Subsystemelement 1
DC1: Diagnosedeckungsgrad für Subsystemelement 1

λ_{De2}: Rate gefährlicher Fehler von Subsystemelement 2
DC2: Diagnosedeckungsgrad für Subsystemelement 2

$\lambda_{DssD} = (1 - \beta)^2 \{[\lambda_{De1} * \lambda_{De2} * (DC1 + DC2)] * T2/2 + [\lambda_{De1} * \lambda_{De2} * (2 - DC1 - DC2)] * T1/2 \} + \beta * (\lambda_{De1} + \lambda_{De2})/2$

$PFH_{DssD} = \lambda_{DssD} * 1h$

Die Subsystemelemente beider Kanäle sind gleich:

λ_{De}: Rate gefährlicher Fehler von Subsystemelement 1 oder 2
DC: Diagnosedeckungsgrad für Subsystemelement 1 or 2

$\lambda_{DssD} = (1 - \beta)^2 \{[\lambda_{De}^2 * 2 * DC] * T2/2 + [\lambda_{De}^2 * (1 - DC)] * T1\} + \beta * \lambda_{De}$

$PFH_{DssD} = \lambda_{DssD} * 1h$

Strukturelle Einschränkungen eines Subsystems

Die strukturellen Einschränkungen fordern ein Minimum an Fehlertoleranz abhängig von der Art der möglichen Fehler des Subsystems. Je größer der Anteil „sicherer" Fehler, desto kleiner ist die geforderte Fehlertoleranz für einen bestimmten SIL.

Bild 2/23 zeigt die entsprechenden Grenzen. „Sichere Fehler" in diesem Zusammenhang sind auch die potentiell gefährlichen Fehler, die durch Diagnose aufgedeckt werden.

Anteil sicherer Fehler	Harwarefehlertoleranz	
	0	1
< 60 %	nicht erlaubt	SIL1
60 % - < 90 %	SIL1	SIL2
90 % - < 99 %	SIL2	SIL3
Anmerkung: Eine Hardwarefehlertoleranz von N bedeutet, dass N+1 Fehler zum Verlust der Funktion führen können.		

Bild 2/23
Strukturelle Einschränkungen eines Subsystems (Auszug aus IEC 62061)

So ist beispielsweise für ein Subsystem, das für SIL 2 eingesetzt werden soll, keine Fehlertoleranz gefordert (FT = 0) wenn der Anteil seiner Fehler, die in eine sichere Richtung gehen, mehr als 90% beträgt. Die meisten Geräte erreichen diesen Wert von sich aus nicht. Man kann aber den Anteil der gefährlichen Fehler verringern, indem man die Fehler durch Diagnose aufdeckt und rechtzeitig eine geeignete Reaktion veranlasst.

Die safe failure fraction eines Subsystems ist der prozentuale Anteil der Fehler, die zu einem sicheren Zustand der Maschine führen, an der Menge aller Fehler des Subsystems gewichtet nach deren Auftretenswahrscheinlichkeit

Definitionen in IEC 62061

Anteil sicherer Fehler (SFF)
Anteil von der gesamten Rate eines Subsystems, der nicht zu einem gefährlichen Ausfall führt.
Die Safe failure fraction (SFF) kann mit folgender Formel berechnet werden:

$(\Sigma\lambda_S + \Sigma\lambda_{DD}) \ / \ (\Sigma\lambda_S + \Sigma\lambda_D)$

dabei ist

λ_S die Rate sicherer Ausfälle,

$\Sigma\lambda_S + \Sigma\lambda_D$ die Gesamtausfallrate,

λ_D die Rate der gefährlichen Ausfälle und

λ_{DD} die Rate der gefährlichen Ausfälle, die durch die Diagnose aufgedeckt werden.

Wenn für ein Gerät nur dessen Gesamtausfallrate angegeben ist, aber die einzelnen Fehlermodi nicht aufgeschlüsselt sind, bietet Anhang D von IEC 62061 Hilfe. In der Tabelle sind typische Werte für Anteile der Fehlermodi für die gebräuchlichsten Gerätetypen angegeben. Welcher Fehlermodus zu einem sicheren oder gefährlichen Ausfall der Sicherheitsfunktion führen kann, ist anwendungsabhängig.

Auswahl der Geräte

Um Geräte in sicherheitsrelevanten Subsystemen verwenden zu können, müssen deren Eigenschaften und Verwendungsbedingungen beschrieben sein.

Zur Beschreibung der sicherheitsspezifischen Eigenschaften sind zusätzlich die folgenden Informationen notwendig:

- Die Ausfallrate und die möglichen Fehlermodi.
  Hinweis: Für elektromechanische Geräte wird die Ausfallrate als B10 Wert angegeben. (Der B10 Wert ist die Anzahl Schaltbeispiele nach der 10% der Geräte ausgefallen sind. Siehe dazu auch IEC 6810-2). Wegen der Häufigkeit einzelner Fehlermodi siehe auch IEC 62061 Anhang D.

- Eigenschaften, die zur Diagnose genutzt warden können (z.B. zwangsgeführte Hilfskontakte).

Subsystem Realisierung

Jedes Subsystem ist so wie im Entwurf festgelegt für seine spezifizierten Eigenschaften und Umgebungsbedingungen zu realisieren. Wenn das Subsystem zudem entsprechend den Anforderungen in IEC 62061 zur Vermeidung und Beherrschung systematischer Fehler realisiert wird, ist es bezüglich seiner „systematischen Integrität“ für die Verwendung in Sicherheitsfunktionen bis SIL 3 geeignet. Es erfüllt ein SIL claim limit SILCL = 3.

2.6 Entwurf und Realisierung der sicherheitsbezogenen Teile einer Steuerung nach EN 954-1 (ISO 13849-1 (rev))

Zielsetzung: Ein sicherheitsrelevantes (Steuerungs-) System muss eine Sicherheitsfunktion korrekt ausführen. Auch im Fehlerfall muss sie sich so verhalten, dass die Maschine oder Anlage in einen sicheren Zustand bleibt oder gebracht wird.

Ermittlung der notwendigen Safety Performance (Safety Integrity)

Durch den Prozess der Risikobeurteilung (siehe Kap. 2.3 „Hängt die Schutzmaßnahme von einer Steuerung ab?“) wurden die Anforderungen an die Sicherheitsfunktion ermittelt.
Die EN 954-1 schreibt eine Kategorie für den Entwurf vor und die Nachfolgenorm ISO 13849-1 (rev) einen erforderlichen Performance Level PL_r. Siehe dazu Kapitel 2.3 „Hängt die Schutzmaßnahme von einer Steuerung ab?“.

Entwurfsprozess der sicherheitsbezogenen Teile einer Steuerung

Die Kategorien nach EN 954-1 beziehen sich gleichermaßen auf das System (Sicherheitsfunktion) und seine Teilsysteme (sicherheitsbezogene Teile einer Steuerung). Bei der Realisierung nach EN 954 kann das gleiche Prinzip der Strukturierung des sicherheitsrelevanten Systems angewendet werden wie in der IEC 62061 beschrieben.

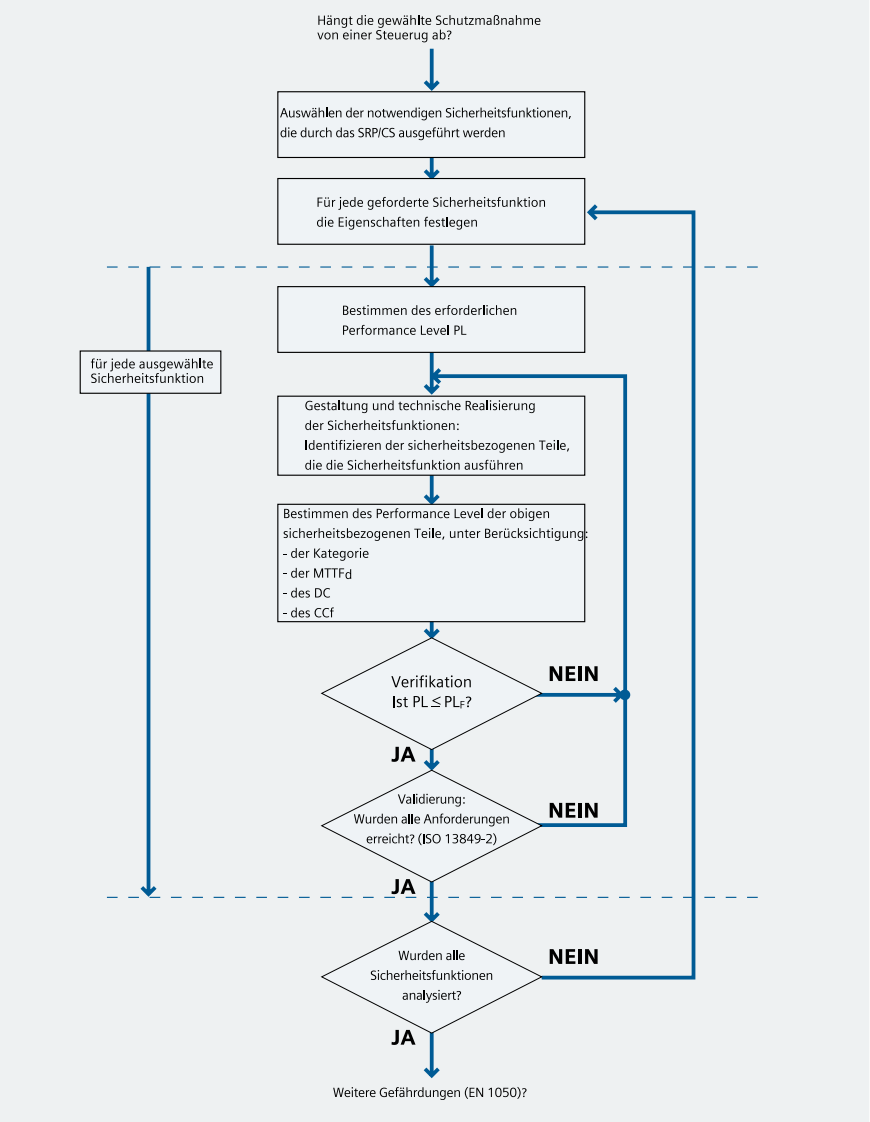

Hängt die gewählte Schutzmaßnahme von einer Steuerug ab?
Auswählen der notwendigen Sicherheitsfunktionen, die durch das SRP/CS ausgeführt werden
Für jede geforderte Sicherheitsfunktion die Eigenschaften festlegen
für jede ausgewählte Sicherheitsfunktion
Bestimmen des erforderlichen Performance Level PL
Gestaltung und technische Realisierung der Sicherheitsfunktionen: Identifizieren der sicherheitsbezogenen Teile, die die Sicherheitsfunktion ausführen
Bestimmen des Performance Level der obigen sicherheitsbezogenen Teile, unter Berücksichtigung:
- der Kategorie
- der MTTFd
- des DC
- des CCf
Verifikation Ist PL ≤ PLr?
NEIN
JA
Validierung: Wurden alle Anforderungen erreicht? (ISO 13849-2)
NEIN
JA
Wurden alle Sicherheitsfunktionen analysiert?
NEIN
JA
Weitere Gefährdungen (EN 1050)?

Bild 2/24
Iterativer Prozess für die Gestaltung der sicherheitsbezogenen Teile von Steuerungen (SRP/CS)

Jedes so abgegrenzte Teilsystem muss dann die Kategorie erfüllen, die für die Schutzfunktion verlangt wird. Die Anforderungen der betreffenden Kategorie gelten auch für die Verdrahtung der Teilsysteme untereinander.

Verglichen mit IEC 62061 wird beim Entwurf nach EN 954 eine Kategorie anstelle des SIL CL (SIL claim limit) angegeben. Es entfällt die quantitative Betrachtung der Wahrscheinlichkeit gefahrbringender Ausfälle.

Dagegen wird in der ISO 13849-1(rev) beim Entwurf neben den Kategorien zusätzlich der Performance Level PL_r als die quantitative Größe für die Ausfallwahrscheinlichkeit eingeführt.

In der Abbildung 2/24 ist der iterative Prozess für die Gestaltung der sicherheitsbezogenen Teile von Steuerungen (SRP/CS) abgebildet:

Realisierung einer Sicherheitsfunktion

Der Architekturentwurf richtet sich nach der geforderten Kategorie bzw. nach dem erforderlichen Performance Level PL_r.

Entwurf nach EN 954

Die erreichte Kategorie des Systems entspricht der Kategorie seiner eingesetzten Teilsysteme.

Der entscheidende Ansatz in der EN 954-1 ist die Fehleraufdeckung sowie die Fehlerbeherrschung, die mit einer Kategorie realisiert werden können. Denn nur wenn ein Fehler aufgedeckt wird, kann auch explizit eine Reaktion eingeleitet werden: die Qualität der Fehleraufdeckung bestimmt das Maß der Fehlerbeherrschung und definiert somit implizit die Fehlerbeherrschungsmaßnahmen (architektureller Entwurf).

Anmerkung: Werden rechnerbasierte Teilsysteme und Buskommunikation eingesetzt, so müssen diese einen bestimmten SIL nach 61508 erfüllen. Dabei gilt folgende Zuordnung: Ein für SIL 1 geeignetes Teilsystem kann für Kategorie 2 eingesetzt werden und entsprechend SIL 2 für Kategorie 3 oder SIL 3 für Kategorie 4.

Entwurf nach ISO 13849-1(rev)

Das Entwurfskonzept von ISO 13849-1 (rev) basiert auf speziellen vordefinierten Architekturen der sicherheitsrelevanten Teile der Steuerung.

Eine Sicherheitsfunktion kann aus einer oder mehrerer sicherheitsbezogene Teile einer Steuerung (SRP/CS) bestehen.

Eine Sicherheitsfunktion kann auch eine Betriebsfunktion sein, wie z.B. eine Zweihandschaltung zur Einleitung eines Prozesses.

Eine typische Sicherheitsfunktion besteht aus folgenden sicherheitsbezogenen Teilen einer Steuerung:

- Eingang (SRP/CS_a)
- Logik / Bearbeitung (SRP/CS_b
- Ausgang / Energieübertragungselement (SRP/CS_c)
- Verbindungen (i_{ab}, i_{ac}) (z.B. elektrisch, optisch)

Anmerkung: Sicherheitsbezogene Teile bestehen aus einer oder mehreren Komponente(n); Komponenten können aus einem oder mehreren Element(en) bestehen.

Alle Verbindungselemente sind in den sicherheitsbezogenen Teilen enthalten.

Wurden die Sicherheitsfunktionen der Steuerung bestimmt, müssen die sicherheitsbezogenen Teile der Steuerung identifiziert werden. Ebenso muss deren Beitrag zu dem Prozess der Risikominderung (ISO 12100) beurteilt werden.

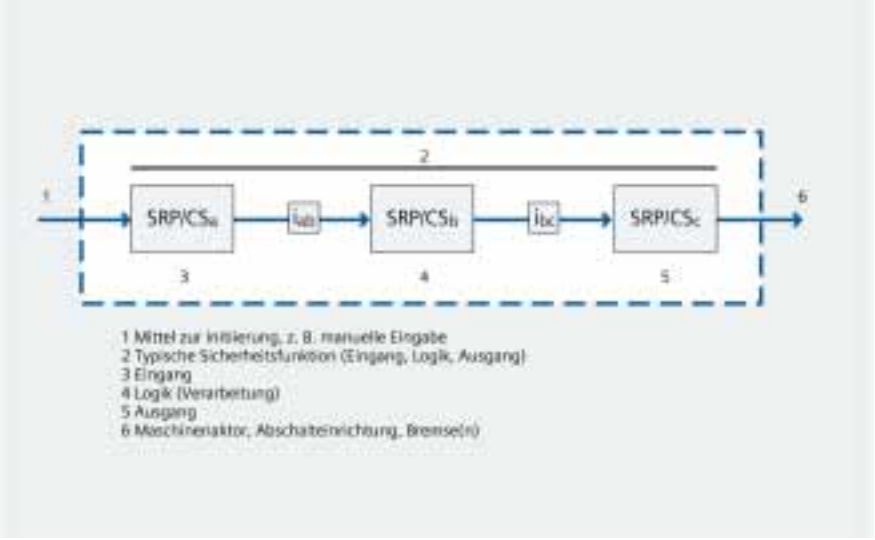


Bild 2/25
Gestaltung einer typischen Sicherheitsfunktion

Entwurf und Realisierung von Kategorien

In der ISO 13849-1(rev) sind die Anforderungen an die Kategorien wie folgt vereinfacht dargestellt:

Kategorie	Zusammenfassung der Anforderungen	Systemverhalten	Prinzipien zum Erreichen der Sicherheit	MTTFd	DC	CCF
B (siehe 6.2.1)	SRP/CSs(en) und/oder ihre Schutzeinrichtungen, als auch ihre Bauteile müssen in Übereinstimmung mit den zutreffenden Normen so gestaltet, gebaut, ausgewählt, zusammengebaut und kombiniert werden, dass sie den zu erwartenden Einflüssen standhalten können.	Das Auftreten eines Fehlers kann zum Verlust der Sicherheitsfunktion führen	Überwiegend durch die Auswahl von Bauteilen charakterisiert	niedrig bis mittel	keine	nicht relevant
1 (siehe 6.2.2)	Die Anforderungen von B müssen erfüllt sein. Bewährte Bauteile und bewährte Sicherheitsprinzipien müssen angewendet werden.	Das Auftreten eines Fehlers kann zum Verlust der Sicherheitsfunktion führen aber die Wahrscheinlichkeit des Auftretens ist geringer als in Kategorie B	Überwiegend durch die Auswahl von Bauteilen charakterisiert	hoch	keine	nicht relevant
2 (siehe 6.2.3)	Die Anforderungen der Kategorie B und die Verwendung bewährter Sicherheitsprinzipien müssen erfüllt sein. Die Sicherheitsfunktion muss in geeigneten Zeitabständen durch die Maschinensteuerung getestet werden.	Das Auftreten eines Fehlers kann zum Verlust der Sicherheitsfunktion zwischen den Tests führen. Der Verlust der Sicherheitsfunktion wird durch den Test erkannt.	Überwiegend durch die Struktur charakterisiert	niedrig bis hoch	niedrig bis mittel	siehe Anhang F
3 (siehe 6.2.4)	Die Anforderungen der Kategorie B und die Verwendung bewährter Sicherheitsprinzipien müssen erfüllt sein. Sicherheitsbezogene Teile müssen so gestaltet werden, dass: - ein einzelner Fehler in jedem dieser Teile nicht zum Verlust der Sicherheitsfunktion führt, und - wenn immer in angemessener Weise durchführbar, der einzelne Fehler erkannt wird.	Wenn ein einzelner Fehler auftritt, bleibt die Sicherheitsfunktion immer erhalten. Einige, aber nicht alle Fehler werden erkannt. Eine Anhäufung von unerkannten Fehlern kann zum Verlust der Sicherheitsfunktion führen.	Überwiegend durch die Struktur charakterisiert	niedrig bis hoch	niedrig bis mittel	siehe Anhang F
4 (siehe 6.2.5)	Die Anforderungen der Kategorie B und die Verwendung bewährter Sicherheitsprinzipien müssen erfüllt sein. Sicherheitsbezogene Teile müssen so gestaltet werden, dass: - ein einzelner Fehler in jedem dieser Teile nicht zum Verlust der Sicherheitsfunktion führt, und - der einzelne Fehler bei oder vor der nächsten Anforderung der Sicherheitsfunktion erkannt wird. Wenn diese Erkennung nicht möglich ist, darf eine Anhäufung von unerkannten Fehlern nicht zum Verlust der Sicherheitsfunktion führen.	Wenn ein einzelner Fehler auftritt, bleibt die Sicherheitsfunktion immer erhalten. Die Erkennung von Fehleranhäufungen reduziert die Wahrscheinlichkeit des Verlustes der Sicherheitsfunktion (hohe DC). Die Fehler werden rechtzeitig erkannt, um einen Verlust der Sicherheitsfunktion zu verhindern.	Überwiegend durch die Struktur charakterisiert	hoch	hoch, einschl. der Fehleranhäufung	siehe Anhang F

Als Beispiel einer vorgesehenen Architektur sei die Kategorie 3 im Anhang B der ISO 13849-1(rev) an dieser Stelle angeführt:

- I1 und I2: Sensor 1 und 2 (z.B. zwei Positionsschalter mit zwangsöffnenden Kontakten)
- L1 und L2: Logikeinheit 1 und 2 (ein Sicherheitsschaltgerät z.B. beinhaltet bereits diese beiden Einheiten)
- O1 und O2: Aktor 1 und 2 (z.B. zwei Schütze)

Die strukturellen Eigenschaften sind:

- Ein redundanter Aufbau
- Die Überwachung der Sensoren (Diskrepanzüberwachung)
- Die Überwachung der Freigabekreise (Überwachung, vergleichbar mit den Rückführkreisen heute)

Diese Architektur wird heute bereits in der Praxis bei Anwendung der EN 954-1 realisiert.

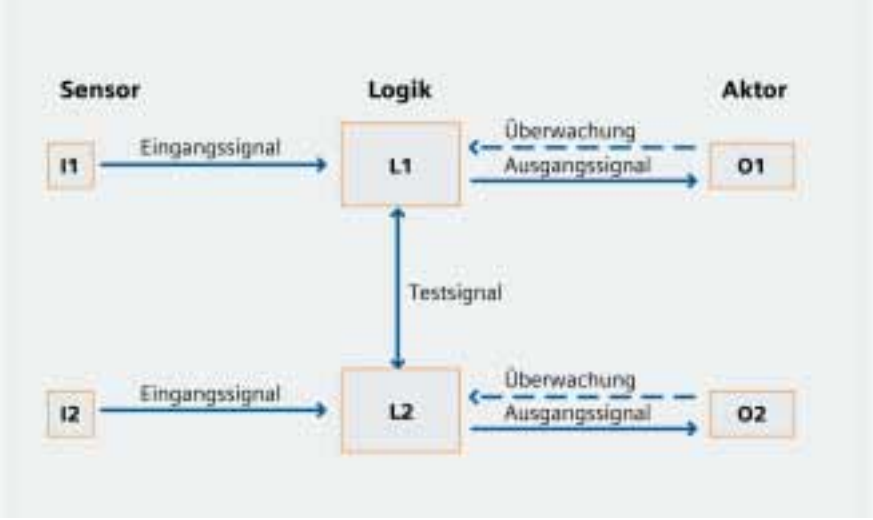
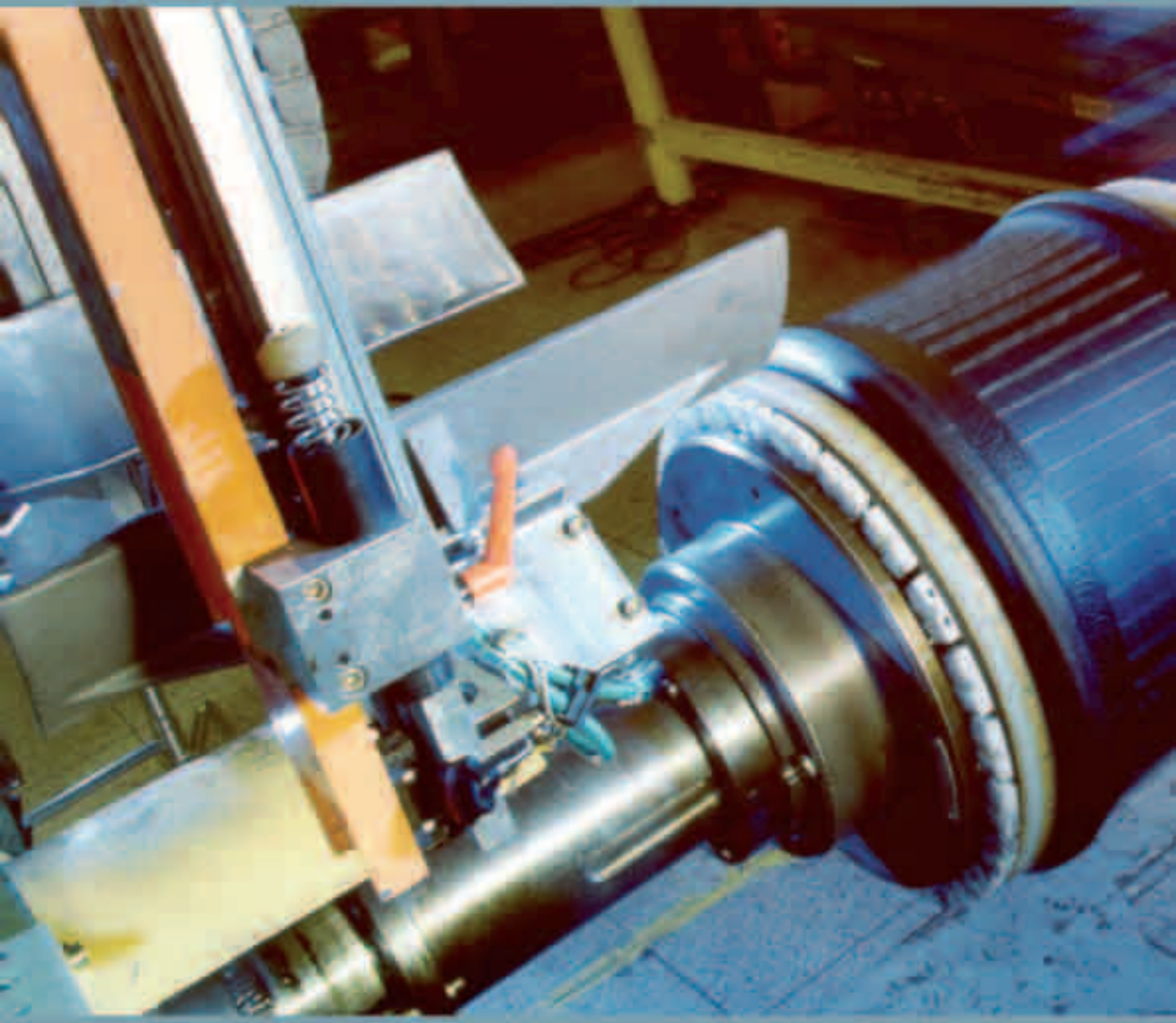


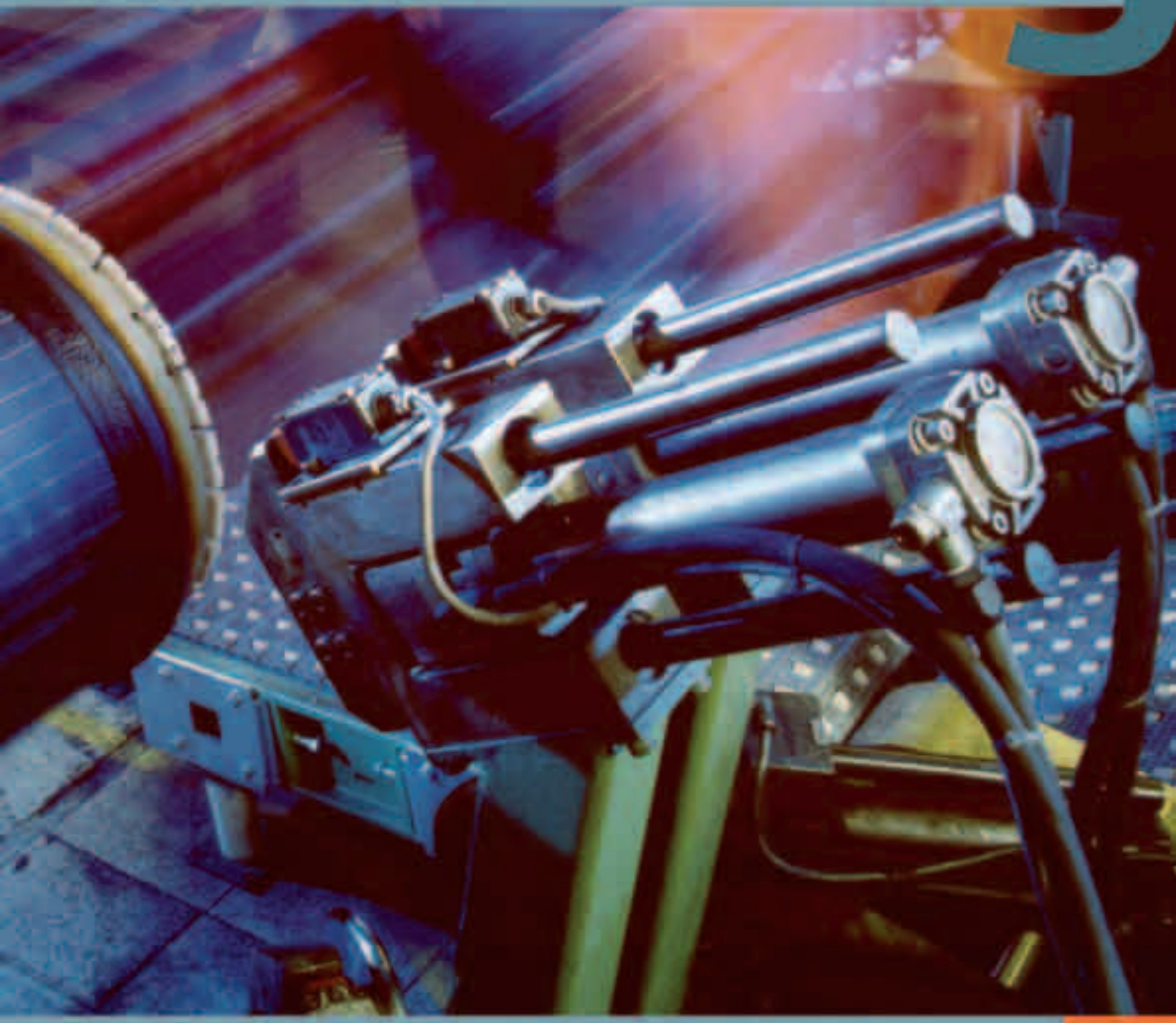
Bild 2/26
Vorgesehene Architektur der Kategorie 3 nach ISO 13849-1(rev)



3.1 Überblick
3.2 Merkmale
3.3 Normen im Überblick
3.4 Sensor/Aktor Anbindung

Sensor-/Aktoreinbindung

3



3 Sensor-/Aktoreinbindung

3.1 Überblick

Das Kapitel Sensor-/Aktor Einbindung zeigt auf, wie die einzelnen Komponenten zu einem System zusammengefügt werden.

Es beruht auf den drei Bereichen:

Erfassen, Auswerten und Reagieren

Mit Erfassen meint man das Einlesen von sicherheitsgerichteten Signalen von z.B. Not-Halt-Tastern oder Lichtvorhänge in eine sichere Auswerteeinheit.

Die Auswerteeinheit wie z.B. S7 F-CPU, SINUMERIK 840D Safety Integrated, ASIsafe Sicherheitsmonitor, Safety Unit oder Sicherheitsschaltgeräte 3TK28 verarbeiten diese Signale, übernehmen die notwendige Fehleraufdeckung und geben Signale gemäß ihrer Abschaltlogik zum Reagieren weiter.

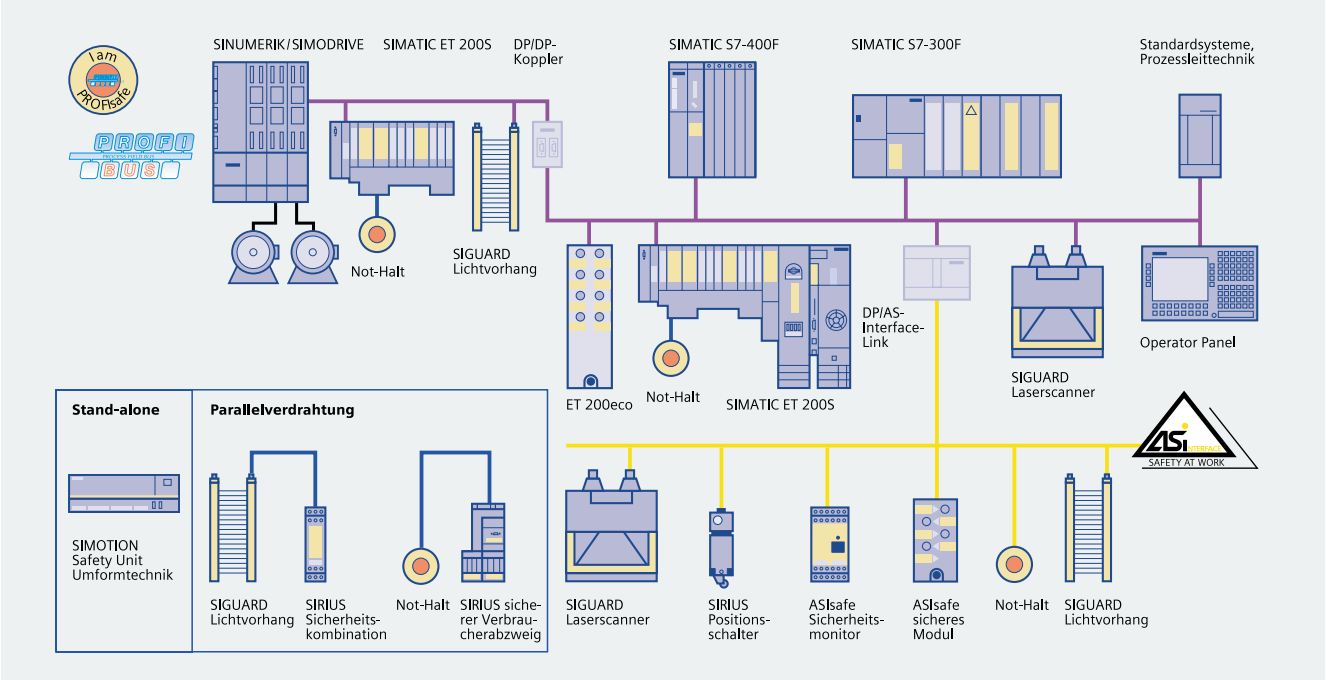
Reagiert wird über interne oder externe Schaltglieder (Aktoren).

Die hier gezeigten Beispiele sind allgemein gehalten, so dass der Anwender unabhängig vom gewählten Auswertegerät eine Lösung finden und gezielt umsetzen kann.

Dieses Kapitel zeigt eine Auswahl von gängigen Schaltungen.

Die Praxis lässt weitere Möglichkeiten zu.

Es wird eine Auswahl der meist verwendeten Schaltungsbeispiele gezeigt.



3.2 Merkmale

Sensoren und Aktoren werden an verschiedene Auswerteeinheiten angeschlossen.

Folgende Varianten sind mit Safety Integrated möglich:

Konventionelle Lösung

- SIRIUS Safety Integrated
  - Sicherheitsschaltgeräte 3TK28..
  - sichere Verbraucherabzweige 3RA7..
  - Sicherheitsauswertegeräte 3RG7848.. für optische Sicherheitssensoren

Busbasierte Lösungen

ASIsafe

- SIRIUS Safety Integrated
  - Sicherheitsmonitor 3RK11..
  - Kompaktmodule K45F und K60F (IP67)
  - Direktanbindung der elektromechanischen Sensoren (IP67)
  - Slimline Module S22.5F (IP20)
- Direktanbindung der optischen Sicherheitssensoren

PROFIsafe

- SIMATIC Safety Integrated
  - CPU S7-300 F
  - CPU S7-400 F
  - Peripherie ET 200S, ET 200M und ET 200eco
- SIRIUS Safety Integrated
  - ET 200S Motorstarter
- SINUMERIK
  - über getrennte Eingangs- /Ausgangs-Hardware E/A von PLC und NC oder über PROFIsafe mit den Peripheriebaugruppen ET 200S und ET 200eco mit der Steuerung SINUMERIK 840D/ SIMODRIVE 611D
- Direktanbindung der optischen Sicherheitssensoren

Mögliche Ausführung der Sensoren

1. Öffner/Öffner Kontakte (äquivalent) → (zwangsöffnende Kontakte)
Diese Variante wird vorwiegend zum Abschalten eingesetzt z.B. bei einer Not-Halt oder Schutztür Überwachung.

2. Schließer/Schließer Kontakte (äquivalent)
Diese Variante wird vorwiegend zum Einschalten eingesetzt, z.B. bei einem Einrichtbetrieb.

3. Öffner/Schließer Kontakte (antivalent)
Diese Variante wird sowohl zum Abschalten als auch zum Einschalten eingesetzt, z.B. Zweihandbedienung.

3.3 Normen im Überblick

Die in diesem Kapitel aufgeführten und dargestellten Informationen bzgl. der Normen werden ausführlich in Kapitel 1 und 2 behandelt.

EN 954-1

Mit den Kategorien (B, 1 bis 4) wird das notwendige Verhalten von sicherheitsbezogenen Teilen einer Steuerung hinsichtlich ihrer Widerstandfähigkeit gegenüber möglichen gefährlichen Fehlern (Fehleraufdeckung, Fehlerbeherrschung) beschrieben.

ISO 13849-1 (rev.)

Die EN 954-1 wird derzeit in einem Entwurf „ISO 13849-1 (rev.)" überarbeitet. Folgende Neuerungen der EN 954-1 „Sicherheit von Maschinen - Sicherheitsbezogene Teile von Steuerungen": 1996 werden vorgeschlagen:

- Der Begriff „Performance Level" verwendet Ausfallwahrscheinlichkeiten ähnlich dem SIL nach IEC 61508. Damit erhält auch die ISO 13849-1 eine quantifizierte und hierarchische Abstufung der Safety Performance: anstelle des deterministischen Ansatzes der EN 954-1 wird nun auch eine probabilistische Methodik eingeführt.
- Die Kategorien 1 bis 4 werden um zusätzliche Berechnungen von Ausfallwahrscheinlichkeiten mit einem Performance Level (PL) ergänzt.

Das Designkonzept von ISO 13849-1 (rev.) basiert auf speziell vordefinierten Architekturen der „sicherheitsrelevanten Teile der Steuerung" (im informativen Annex B als „designated architecture" bezeichnet).

Auf weitergehende Erläuterungen des Konzeptes nach ISO 13849-1 (rev.) wird an dieser Stelle verzichtet, da dieses derzeit noch überarbeitet wird.

IEC 61508

Die IEC 61508 „Funktionale Sicherheit sicherheitsbezogener elektrischer, elektronischer, programmierbarer elektronischer System" ist die Basisnorm, auf die die IEC 62061 aufbaut.

IEC 62061

Die IEC 62061 „Sicherheit von Maschinen – Funktionale Sicherheit von elektrischen, elektronischen und programmierbaren Steuerungen von Maschinen" gilt als „Stand der Technik" und konzentriert sich vorwiegend auf die Anforderungen, die der Maschinenhersteller bei Entwurf und Realisierung sicherheitsrelevanter elektrischer Steuerungen erfüllen muss.

Sie beschreibt, wie ein System aus vorhandenen Teilsystemen aufgebaut wird und wie die erreichte Safety Performance bestimmt werden kann: SIL, Sicherheitsintegritäts-Level (Safety Integrity Level), wird als Maß für die „Sicherheitsleistungsfähigkeit" (Safety Performance) herangezogen.

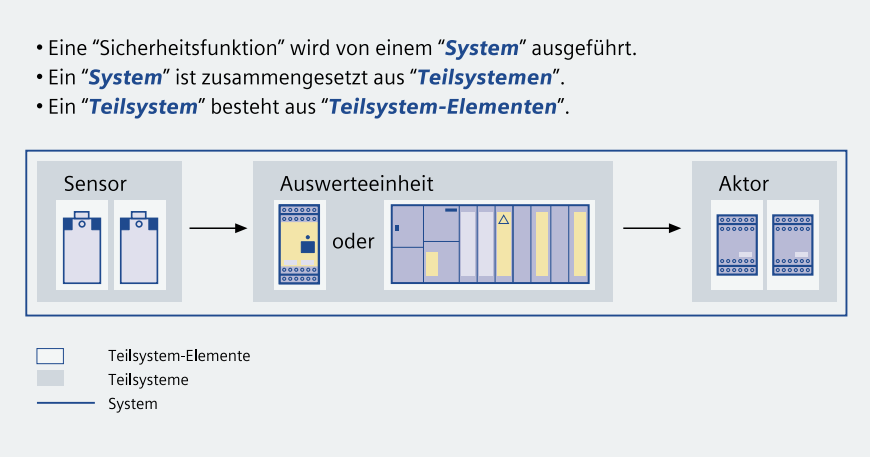


Bild 3/1
System, Teilsystem und Teilsystemelemente nach IEC 62061

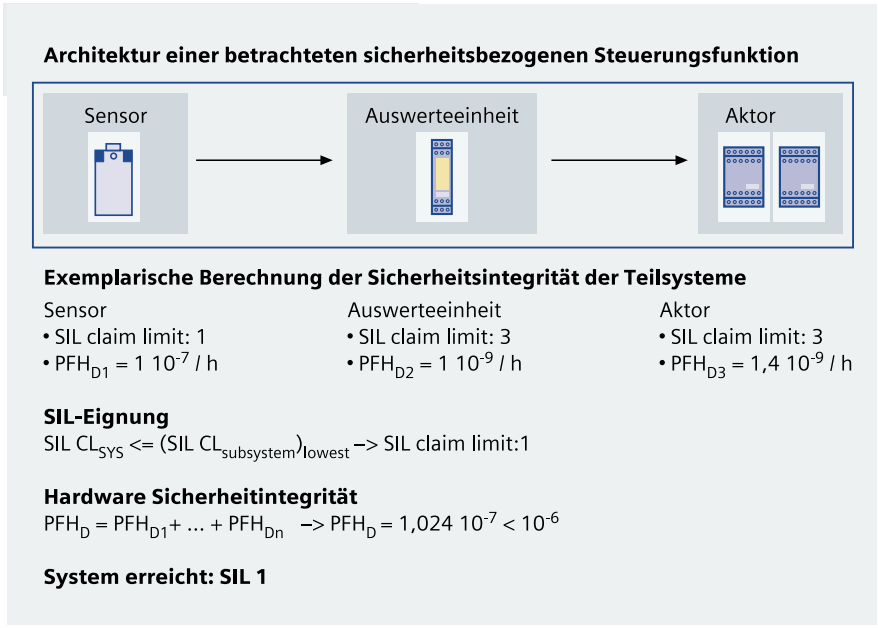

Architektur einer betrachteten sicherheitsbezogenen Steuerungsfunktion
Sensor
Auswerteeinheit
Aktor
Exemplarische Berechnung der Sicherheitsintegrität der Teilsysteme
Sensor
• SIL claim limit: 1
• PFH$_{D1}$ = 1 10^{-7} / h
Auswerteeinheit
• SIL claim limit: 3
• PFH$_{D2}$ = 1 10^{-9} / h
Aktor
• SIL claim limit: 3
• PFH$_{D3}$ = 1,4 10^{-9} / h
SIL-Eignung
SIL CL$_{SYS}$ <= (SIL CL$_{subsystem}$)$_{lowest}$ –> SIL claim limit:1
Hardware Sicherheitintegrität
PFH$_D$ = PFH$_{D1}$+ ... + PFH$_{Dn}$ –> PFH$_D$ = 1,024 10^{-7} < 10^{-6}
System erreicht: SIL 1

Bild 3/2
Anwendungsbeispiel für die Anwendung nach der IEC 62061

Der SIL claim limit beschränkt den erreichbaren SIL des Systems (Sicherheitsfunktion), obwohl die „Random Integrity (Sicherheitsintegrität gefahrbringender zufälliger Hardwareausfälle)"den SIL 2 erreicht.

Die Applikation in Bild 3/2 besteht aus folgenden Teilsystemen:

- Erfassen (ein Positionsschalter, 1-kanalig)
- Auswerten (3TK28.., mit Diagnose)
- Reagieren (zwei Schütze)

Die zur Berechnung heran gezogenen PFH$_D$ Werte sind beispielhaft und keine Originalwerte.

Prinzipielle Vorgehensweise bei der Anwendung der IEC 62061:

- Die **1. Anforderung (SIL-Eignung der Teilsysteme)** begrenzt die erreichbare „Sicherheitsleistungsfähigkeit" (Safety Performance) des Systems.

  SILSYSTEM <= SILCLlowest

Jedes Teilsystem ist aufgrund seiner systematischen Eigenschaften nur bis zu einem bestimmten SIL geeignet. Dieser Wert begrenzt den möglichen SIL des Systems (schwächstes Glied der Kette).

- Die **2. Anforderung (Hardware Sicherheitsintegrität)** ist die Begrenzung der Wahrscheinlichkeit „gefährlicher Fehler" für die gesamte Sicherheitsfunktion, d.h. die Summe aller Ausfallwahrscheinlichkeiten aller Teilsysteme darf nicht den PFH$_D$ des geforderten SIL überschreiten.

Die Ausfallwahrscheinlichkeit der Schütze (das elektromechanische Teilsystem „Aktor") wird nach einer vereinfachten Berechnung mit den B10 Werten nach IEC 62061 bestimmt.

Es gilt für das System folgende Gleichung:

PFHD(System) = PFHD(Erfassen) + PFHD(Auswerten) + PFHD(Reagieren) + PTE <= geforderte Ausfallwahrscheinlichkeit des Systems

Bei einer sicherheitsgerichteten Kommunikation muss die Wahrscheinlichkeit möglicher Datenübertragungsfehler (P$_{TE}$) hinzu addiert werden.

- Die **3. Anforderung (Auswahl und Verschaltung)**, es muss bei der Auswahl und Verschaltung der Teilsysteme die entsprechende Anforderung von IEC 62061 6.4 „Anforderungen zur systematischen Sicherheitsintegrität" erfüllt werden.

3.4 Sensor/Aktor Anbindung

Allgemein

Prinzip Kategorie B nach EN 954-1

Die sicherheitsbezogenen Teile von Maschinensteuerungen und/oder ihre Schutzeinrichtungen sowie ihre Bauteile müssen in Übereinstimmung mit den zutreffenden Normen so gestaltet, konstruiert und ausgewählt werden, dass sie den zu erwartenden Umgebungseinflüssen standhalten können.

Durch die stetig steigende Verzahnung und Globalisierung der Wirtschaft wird mit der Kategorie B im Wirtschaftsbereich der EU ein gewisser Mindeststandard festgeschrieben.

Anforderung

Die Steuerung muss so konzipiert sein, dass sie dem zu erwartenden Umgebungseinflüssen standhalten kann.

Systemverhalten

Das Auftreten eines Fehlers kann zum Verlust der Sicherheitsfunktion führen.

Prinzip

Das Erreichen der Sicherheit wird überwiegend durch die Auswahl von Bauteilen, z.B. spritzwassergeschützt, staubgeschützt, vibrationsgeschützt usw. charakterisiert.

Prinzip Kategorie 1 nach EN 954-1

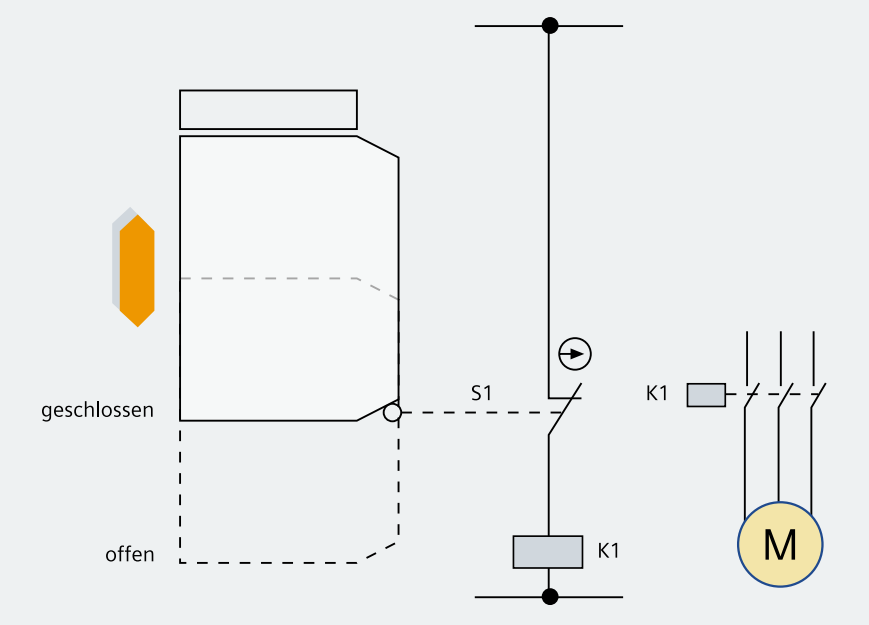


Bild 3/3
Prinzip Kategorie 1 nach EN 954-1 am Beispiel einer Schutztürüberwachung

Beschreibung und zusätzliche Info

Anforderung

Die Anforderung von B muss erfüllt sein; zusätzlich sind sicherheitstechnisch bewährte Bauteile und Prinzipien zu verwenden. Ein Bauteil hat sich bewährt, wenn es in der Vergangenheit mit erfolgreichen Ergebnissen weit verbreitet verwendet worden ist.

Systemverhalten

Das Auftreten eines Fehlers kann zum Verlust der Sicherheitsfunktion führen. Die Wahrscheinlichkeit eines Ausfalls ist in Kategorie 1 geringer als in Kategorie B.

Prinzip

Auswahl von Bauteilen
Sensorik: z.B. gemäß EN 954-1
Aktoren: „bewährte Bauteile“
(z.B. Schütze/Leistungsschalter)

Prinzip Kategorie 2 nach EN 954-1

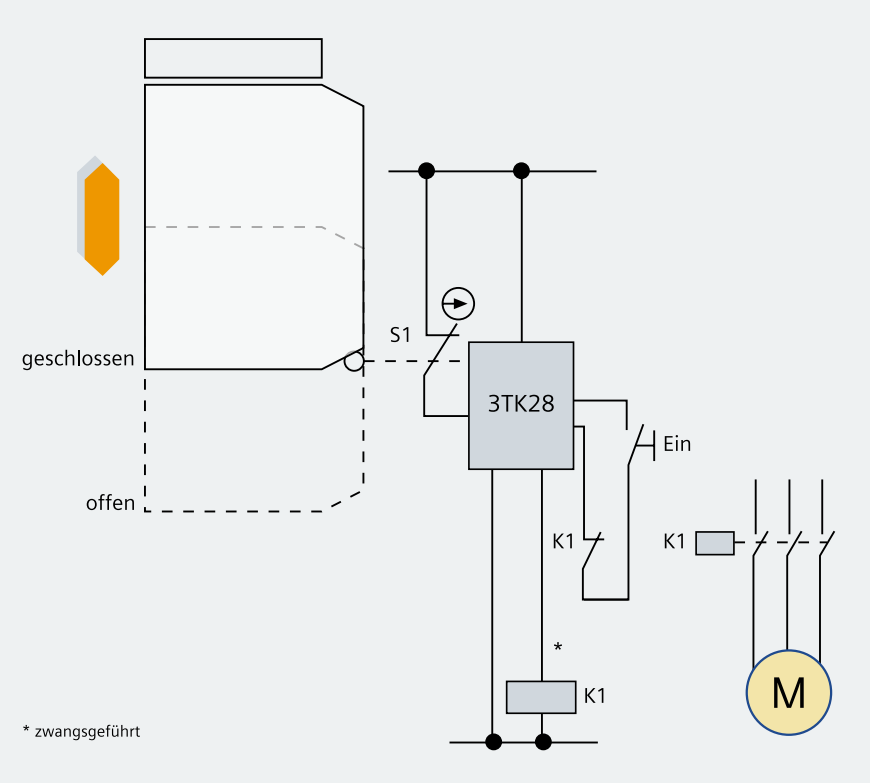


Bild 3/4
Prinzip Kategorie 2 nach EN 954-1 am Beispiel einer Schutztürüberwachung (die „Maschinensteuerung“ ist eine Standard SPS)

Mit diesem Beispiel kann die Kategorie 2 nach EN 954-1 nur dann erfüllt werden, wenn bei dem Versagen des Aktors automatisch eine Warnung erfolgt oder die Maschinensteuerung einen sicheren Zustand einleitet. Ansonsten ist ein zweiter Abschaltweg erforderlich.

Prinzip

Struktur der Steuerung
Fehlererkennung: z.B. durch 3TK28 Sicherheitsschaltgerät oder eine F-Steuerung
Sensorik: z.B. gemäß EN 954-1 bzw. IEC 60947-5-1
Aktoren: „bewährte Bauteile“ (z.B. Schütze)

Beschreibung und zusätzliche Info

Anforderung

Die Anforderung von B und die Verwendung bewährter Sicherheitsprinzipien müssen erfüllt sein. Es sind zusätzliche Prüfungen der Sicherheitsfunktion in geeigneten Zeitabständen (z.B. durch sporadisches Öffnen der Schutztür) durchzuführen.

Systemverhalten

Das Auftreten eines Fehlers kann zum Verlust der Sicherheitsfunktion zwischen den Prüfungsabständen führen. Der Verlust der Sicherheitsfunktion wird durch die Prüfung erkannt. Wird ein Fehler erkannt, muss ein sicherer Zustand bis zur Fehlerbeseitigung aufrechterhalten werden.

Prinzip Kategorie 3 nach EN954-1

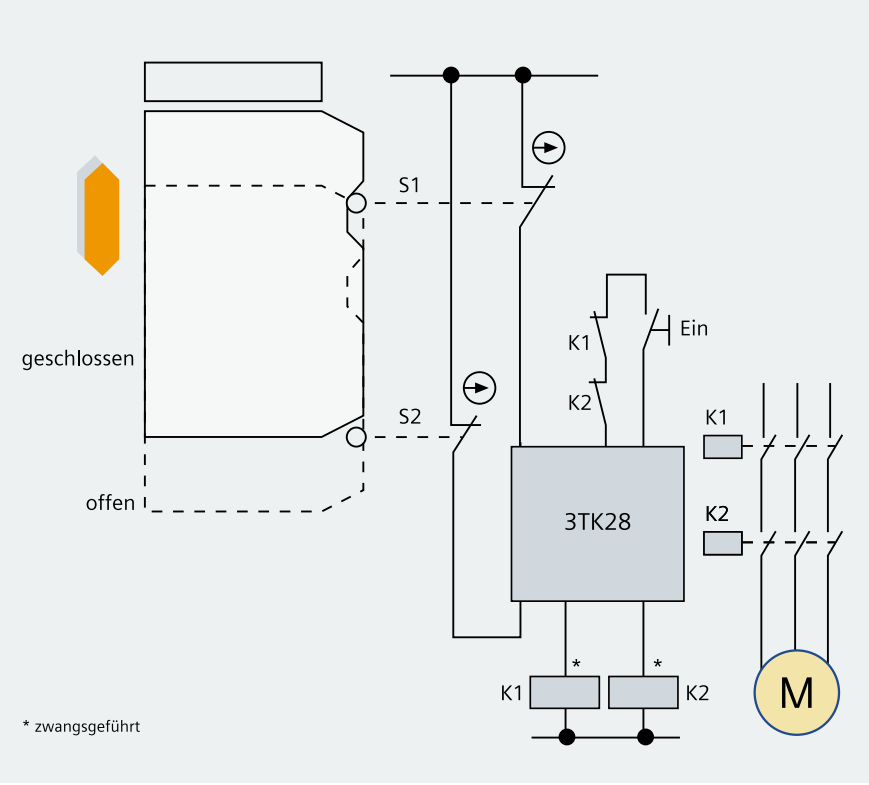


Bild 3/5
Prinzip Kategorie 3 nach EN 954-1 am Beispiel einer Schutztürüberwachung

Beschreibung und zusätzliche Info

Anforderung

Die Anforderung von B und die Verwendung bewährter Sicherheitsprinzipien müssen erfüllt sein. In Kategorie 3 müssen alle sicherheitsbezogenen Teile so gestaltet sein, dass einzelne Fehler nicht zum Verlust der Sicherheitsfunktion führen. Der einzelne Fehler muss bei der nächsten Anforderung der Sicherheitsfunktion erkannt werden. Diese Forderung kann z.B. durch eine Redundanz (siehe Bild3/5) erreicht werden.

Systemverhalten

Wenn ein einzelner Fehler auftritt, bleibt die Sicherheitsfunktion immer erhalten. Einige, aber nicht alle Fehler werden erkannt. Eine Anhäufung unerkannter Fehler kann zum Verlust der Sicherheitsfunktion führen.

Prinzip

Struktur der Steuerung
Fehlererkennung: z.B. durch 3TK28 Sicherheitsschaltgerät oder eine F-Steuerung
Sensorik: redundant ausgeführt
Aktoren: redundant ausgeführt

Prinzip Kategorie 4 nach EN 954-1

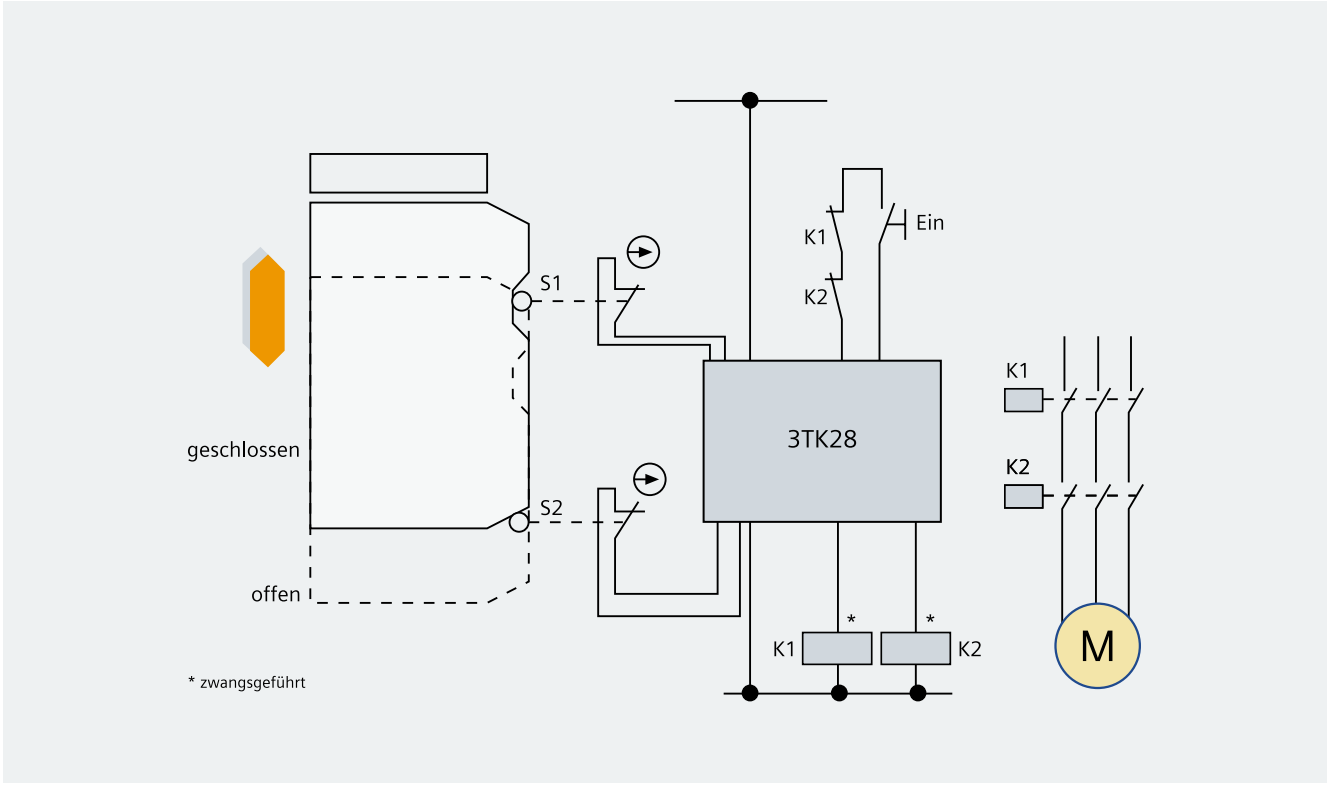


Bild 3/6
Prinzip Kategorie 4 nach EN 954-1 am Beispiel einer Schutztürüberwachung

Anforderung

Die Anforderung von B und die Verwendung bewährter Sicherheitsprinzipien müssen erfüllt sein.

Sicherheitsbezogene Teile nach Kategorie 4 müssen so gestaltet werden, dass ein einzelner Fehler in jedem dieser Teile nicht zum Verlust der Sicherheitsfunktion führt, und der einzelne Fehler bei oder vor der nächsten Anforderung an die Sicherheitsfunktion erkannt wird oder, wenn dies nicht möglich ist, eine Anhäufung von Fehlern dann nicht zu dem Verlust der Sicherheitsfunktion führt. Außerdem müssen Fehler mit gemeinsamer Ursache berücksichtigt werden, z.B. durch das Verhindern von EMV Einflüssen.

Systemverhalten

Wenn Fehler auftreten, bleibt die Sicherheitsfunktion immer erhalten. Die Fehler werden rechtzeitig erkannt, um einen Verlust der Sicherheitsfunktion zu verhindern.

Prinzip

Struktur der Steuerung
Fehlererkennung: z.B. durch 3TK28 Sicherheitsschaltgerät oder eine F-Steuerung und zusätzliche Überwachung, Querschlusserkennung und überwachter Start.
Sensorik: redundant ausgeführt und getaktet
Aktoren: redundant ausgeführt
Die Erhöhung der Sicherheit durch zusätzliche Maßnahmen, wie z.B. durch Überdimensionierung der Lastschütze führt nicht zu einer höheren Kategorie!

Dies führt zu keinem Fehlerausschluss!

Manueller, überwachter Start und Autostart (EN 954-1, EN 60204-1)

Ist mit den verschiedenen Sicherheitskomponenten (Teilsystem Auswertung) möglich.

Ein Sicherheitsgerät kann manuell bzw. überwacht oder automatisch gestartet werden.

Bei einem manuellen oder überwachten Start wird durch das Betätigen des EIN Tasters, nach Prüfung des Eingangsabbildes und nach positivem Test des Sicherheitsgerätes, ein Freigabesignal erzeugt.
Diese Funktion wird auch als statischer Betrieb bezeichnet und ist für Not-Halt-Einrichtungen vorgeschrieben (EN 60204-1, bewusste Handlung).

Der überwachte Start wertet, im Gegensatz zum manuellen Start, ein Signalwechsel des EIN Tasters aus. Somit kann die Bedienung des EIN Tasters nicht überlistet werden.

Bei einem Autostart wird ohne manuelle Zustimmung, aber nach Prüfung des Eingangsabbildes und positivem Test des Sicherheitsschaltgerätes, ein Freigabesignal erzeugt. Diese Funktion wird auch als dynamischer Betrieb bezeichnet und ist für Not-Halt-Einrichtungen unzulässig.

Nicht begehbare trennende Schutzeinrichtungen arbeiten mit dem automatischen Start.

Anmerkung: Der manuelle Start kann mit einem Sicherheitsschaltgerät mit automatischem Start realisiert werden, wenn im Rückführkreis zusätzlich zu den zwangsgeführten Kontakten der Lastschütze ein EIN Taster in Reihe mit eingebunden wird (siehe Bild 3/11).

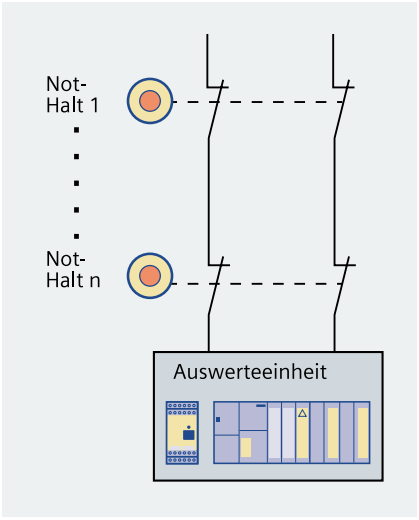


Bild 3/7
Reihenschaltung bis Kategorie 4 nach EN 954-1 am Beispiel Not-Halt Überwachung

Manueller Start ist bis Kategorie 3 nach EN 954-1 möglich.

Der manuelle Start ist bis Kategorie 3 nach EN 954-1 (ISO 13849-1 rev.) für eine Not-Halt-Einrichtung zulässig.

Überwachter Start ist bei Kategorie 4 notwendig.

Der überwachte Start ist bei Kategorie 4 nach EN 954-1 (ISO 13849-1 rev.) für eine Not-Halt-Einrichtung notwendig: ein unerwarteter Anlauf muss ausgeschlossen werden.

Beschreibung und zusätzliche Info

Not-Halt Überwachungen dürfen immer in Reihe geschaltet werden: das Versagen und gleichzeitige Drücken der Not-Halt Befehlsgeräte kann ausgeschlossen werden.

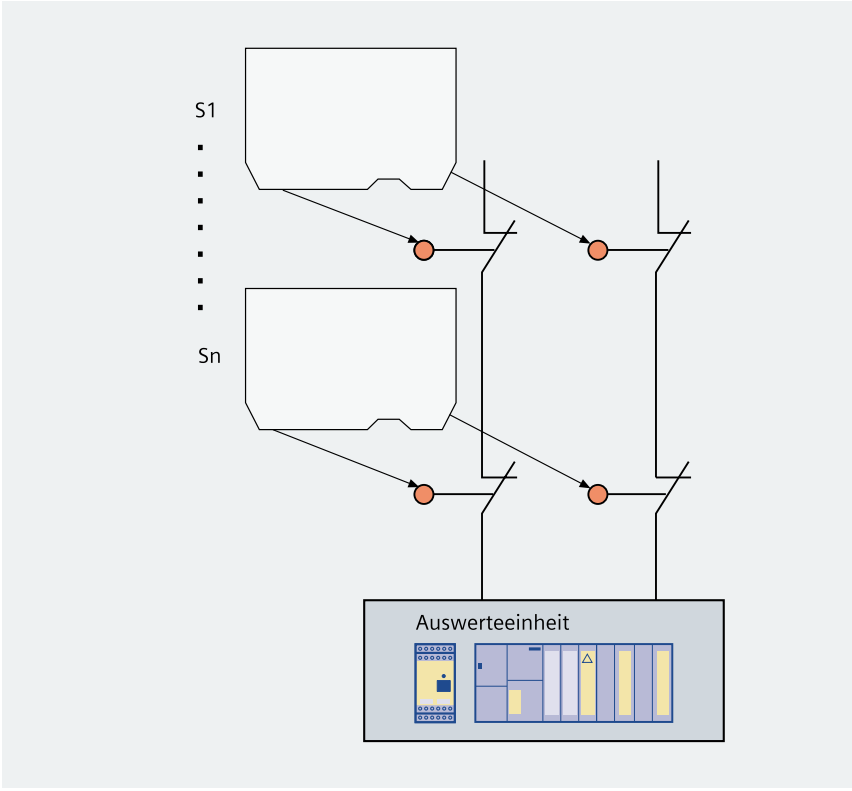


Bild 3/8
Reihenschaltung bis Kategorie 3 nach EN 954-1 am Beispiel Schutztürüberwachung

Beschreibung und zusätzliche Info

- Positionsschalter dürfen bis Kategorie 3 nach EN 954-1 in Reihe geschaltet werden, wenn nicht mehrere Schutztüren regelmäßig gleichzeitig geöffnet werden (da sonst keine Fehleraufdeckung erfolgen kann).
- Positionsschalter dürfen für Kategorie 4 nach EN 954-1 nie in Reihe geschaltet werden, weil immer jeder gefährliche Fehler aufgedeckt werden muss (unabhängig vom Bedienpersonal).

Sichere (geschützte) Verlegung, sichere Trennung nach IEC 61140-1; EN 50187

- Ziel ist die Erreichung einer hohen Betriebssicherheit. Zum Schutz vor Spannungsverschleppung müssen die unterschiedlichen Spannungen in einem Kabel oder Betriebsmittel gegen die höchste vorkommende Spannung isoliert sein (Schutz vor elektrischen Schlag, IEC 61140) Leitungsisolierung zwischen zwei Leitern unterschiedlicher Potenziale.
- ASI Module müssen zwischen AS-Interface und U_{hilf} die Anforderungen gemäß EN 50187 bzgl. der Luft- und Kriechstrecken und der Spannungsfestigkeit der Isolation der relevanten Bauteile erfüllen.

Konventionelle Sensoreinbindung ohne sicherheitsgerichtete Kommunikation über Feldbusse

Beschreibung und zusätzliche Info

Das **Erfassen** erfolgt über mechanische Schalter wie Not-Halt-Taster, Positionsschalter oder Lichtvorhänge, Lichtgitter, Laserscanner.

Die **Auswertung** erfolgt über SIRIUS Sicherheitsschaltgeräte 3TK28. Der sichere Verbraucherabzweig 3RA7 beinhaltet neben der 3TK28 Technik redundante Lastschütze, die als Einheit in Kategorie 4 gemäß EN 954-1 einen Aktor sicher abschalten können.

Reagiert wird direkt über diskrete Schalttechnik (Schütze) oder mit Hilfe von PMD-Fxx Modulen in einer ET 200S Station im Zusammenspiel mit Motorstartern (siehe Bild 3/17) oder Frequenzumrichtern.

Die Applikation Bild 3/10 besteht aus folgenden drei Teilsystemen:

- Erfassen (zwei Positionsschalter jeweils 1-kanalig)
- Auswerten (3TK28.., mit Diagnose)
- Reagieren (zwei Schütze)

Die zur Berechnung heran gezogenen PFH_D Werte sind beispielhaft.

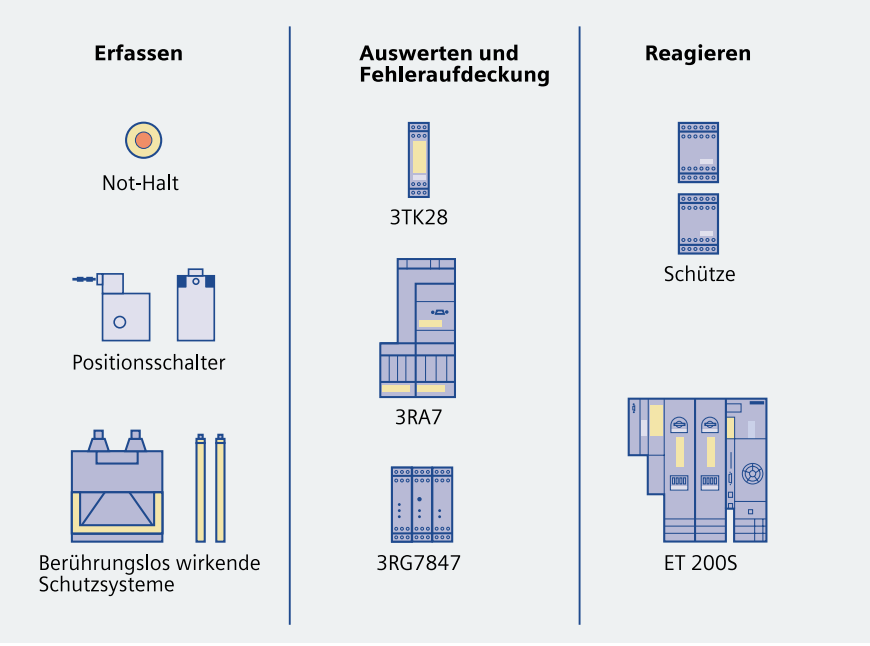


Bild 3/9
Gruppenbild direkte Sensor Einbindung (konventionell)

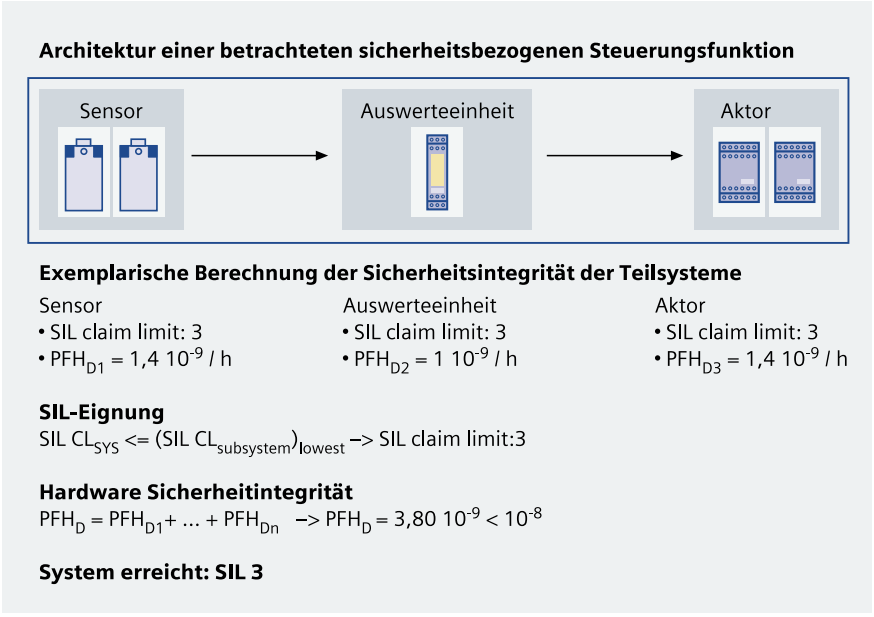

Architektur einer betrachteten sicherheitsbezogenen Steuerungsfunktion
Sensor
Auswerteeinheit
Aktor
Exemplarische Berechnung der Sicherheitsintegrität der Teilsysteme
Sensor
• SIL claim limit: 3
• PFH$_{D1}$ = 1,4 10^{-9} / h
Auswerteeinheit
• SIL claim limit: 3
• PFH$_{D2}$ = 1 10^{-9} / h
Aktor
• SIL claim limit: 3
• PFH$_{D3}$ = 1,4 10^{-9} / h
SIL-Eignung
SIL CL$_{SYS}$ <= (SIL CL$_{subsystem}$)$_{lowest}$ –> SIL claim limit:3
Hardware Sicherheitintegrität
PFH$_D$ = PFH$_{D1}$+ ... + PFH$_{Dn}$ –> PFH$_D$ = 3,80 10^{-9} < 10^{-8}
System erreicht: SIL 3

Bild 3/10
Anwendungsbeispiel für die Anwendung nach der IEC 62061 bei der konventionellen Anbindung ohne sicherheitsgerichtete Kommunikation

Sensor/Aktor Anbindung ohne sicherheitsgerichtete Kommunikation

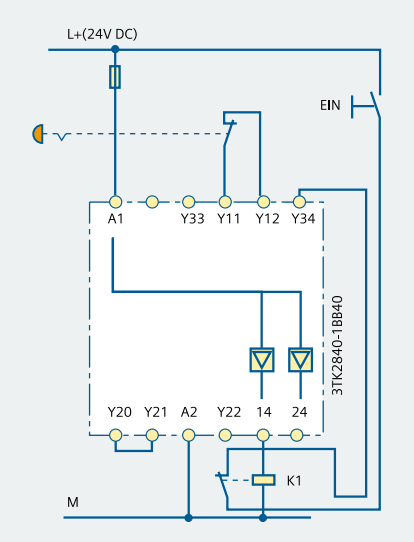


Bild 3/11
SIRIUS Sicherheitsschaltgerät 3TK2840, Not-Halt, Kategorie 2 nach EN 954-1, einkanalig mit Rückführkreis (die Maschinensteuerung ist eine Standard SPS)

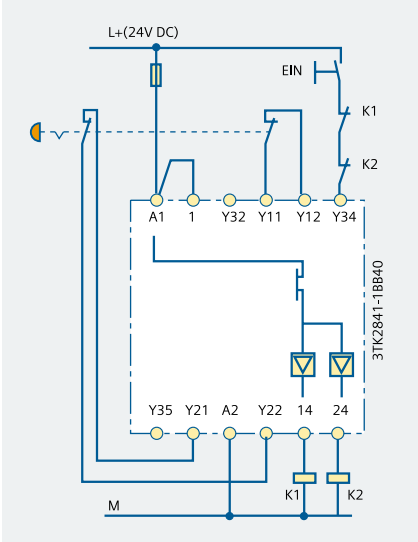
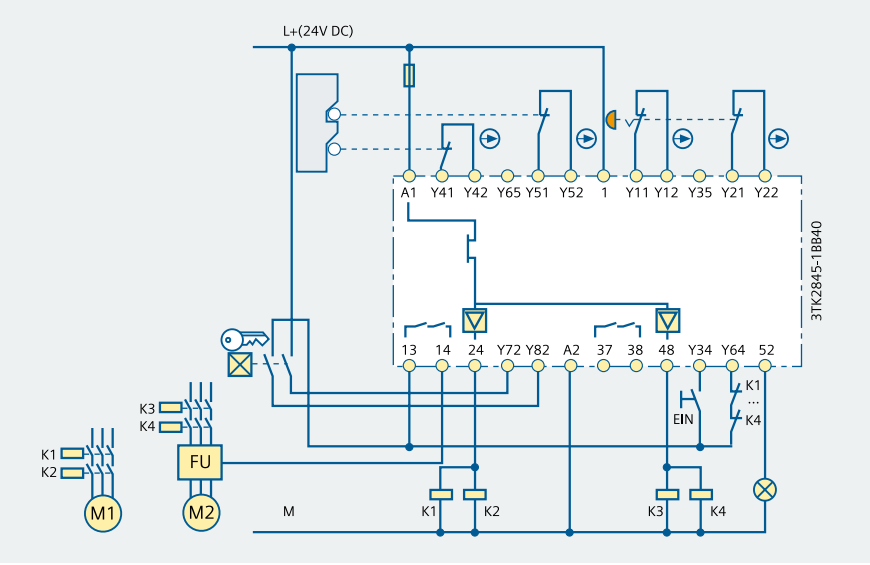


Bild 3/12
SIRIUS Sicherheitsschaltgerät 3TK2841, Not-Halt, Kategorie 4 nach EN 954-1, zweikanalig mit Rückführkreis, überwachter Start mit EIN-Taster

Beschreibung und zusätzliche Info

- Durch Betätigung des in den Rückführkreis eingeschleiften „EIN-Tasters“ werden die Schütze K1 und K2 (Aktoren) zugeschaltet. Wird nun der Not-Halt Taster betätigt, schaltet das Sicherheitsschaltgerät die beiden Schütze (Aktoren) wieder ab.
- Bei einer Kategorie 2 Anwendung ist es ausreichend, wenn der Sensor (hier der Not-Halt Taster) einkanalig ausgewertet, und der Aktor (Lastschütz) einkanalig angesteuert wird.
- Sollte ein Lastschütz fehlerbehaftet sein, z.B. durch das Verschweißen von Kontakten, wird der Rückführkreis auch beim Betätigen des EIN-Tasters nicht geschlossen und das 3TK28 gibt seine Freigabekreise nicht frei (Fehleraufdeckung).

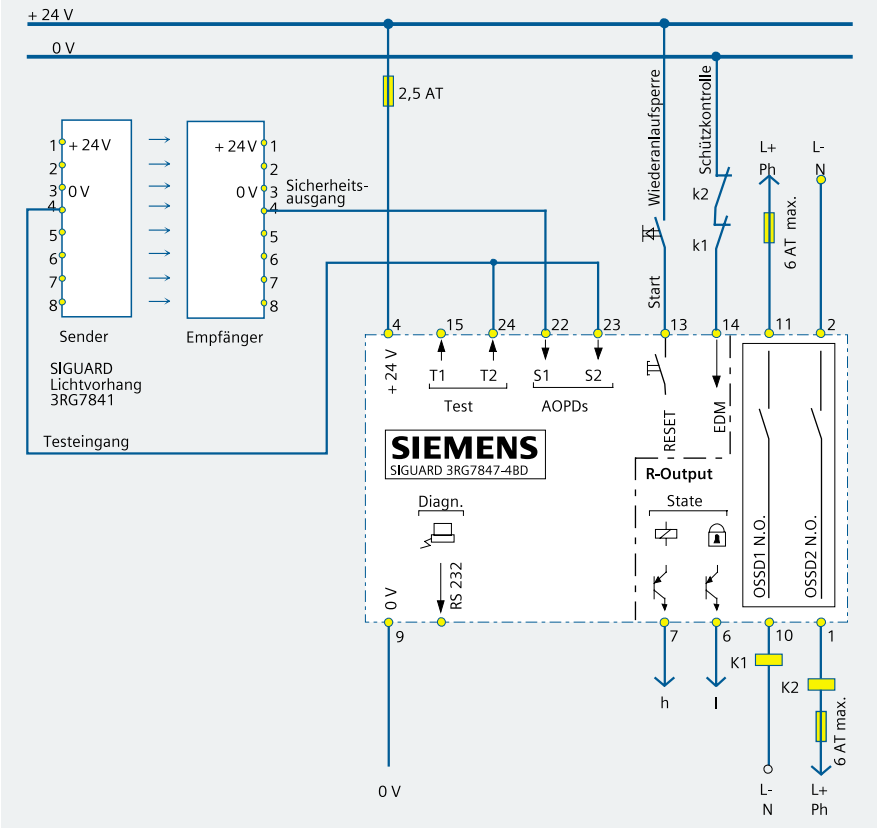


Beschreibung und zusätzliche Info

Mit dem 3TK2845 wird folgendes realisiert:

- Not-Halt mit überwachten Start
- Schutztürüberwachung mit automatischen Start
- Schlüsselschalter, der die Schutztür für den Servicebetrieb überbrückt

Bild 3/13
Not-Halt und Schutztürüberwachung Kategorie 4 nach EN 954-1, mit 3TK2845 in Stop-Kategorie 0 nach EN 60204-1



Beschreibung und zusätzliche Info

- Sensorleitungen sind geschützt zu verlegen; als Sensoren sind ausschließlich Sicherheitssensoren mit zwangsöffnenden Kontakten zu verwenden.
- Bei Typ 2 Schutzeinrichtungen wird die Schutzwirkung durch eine periodische Testung überprüft. Diese Testroutine übernimmt hier das Auswertegerät 3RG7847...

Bild 3/14
SIGUARD 3RG7841.., Lichtvorhangüberwachung, Typ 2 nach IEC 61496-1, 2 bzw. EN 61496-1, 2, einkanalig an Auswertegerät 3RG7847-4BD, manueller Start und Rückführkreis

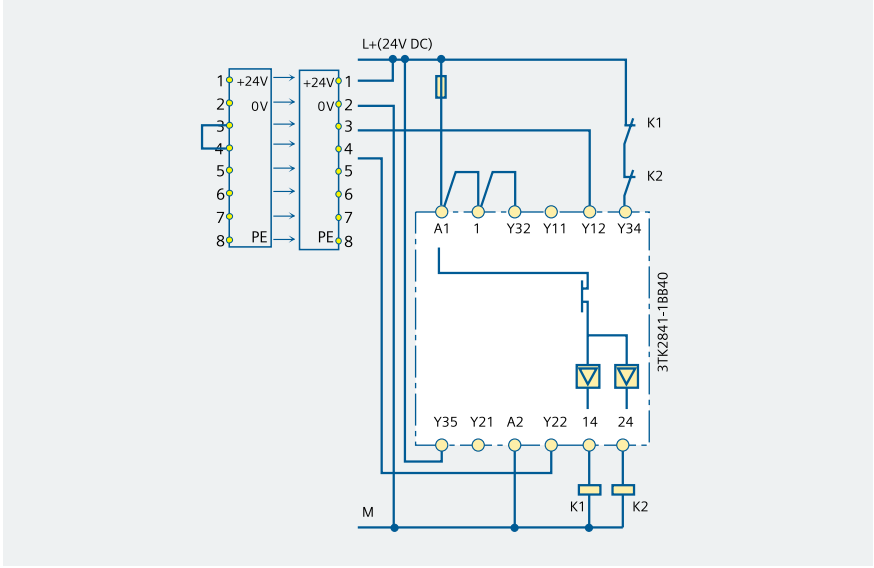


Bild 3/15
SIGUARD 3RG7842.., Lichtvorhang/-gitterüberwachung, Typ 4 nach IEC 61496-1, 2, zweikanalig an SIRIUS 3TK284.., Stop-Kategorie 0, nach EN 60204-1, Autostart und Rückführkreis

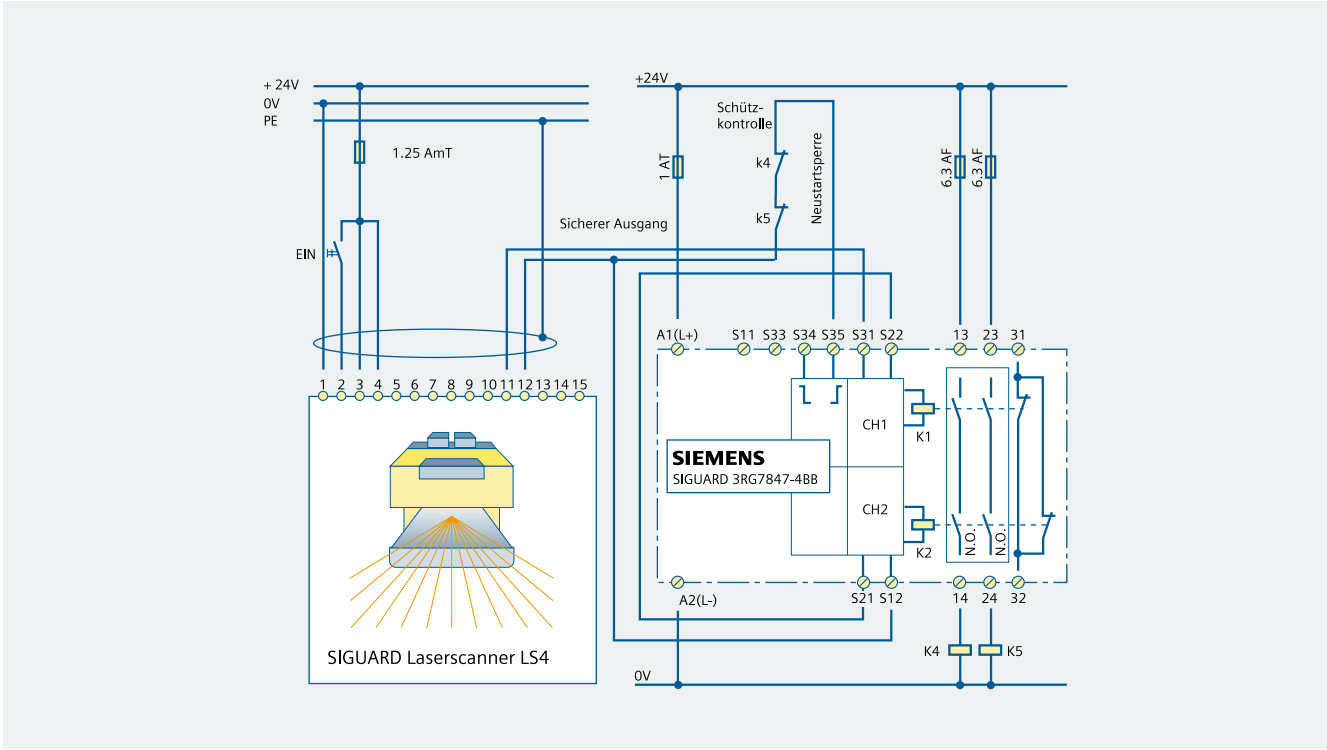


Bild 3/16
SIGUARD Laserscanner LS4, Typ 3 nach IEC 61496-1, 2 bzw. EN 61496-1, 2 zweikanalig, an 3RG7847-4BB, (Auswerteeinheit)
Laserscanner konfiguriert auf manuellen Start, Rückführkreisüberwachung durch 3RG7847-4BB

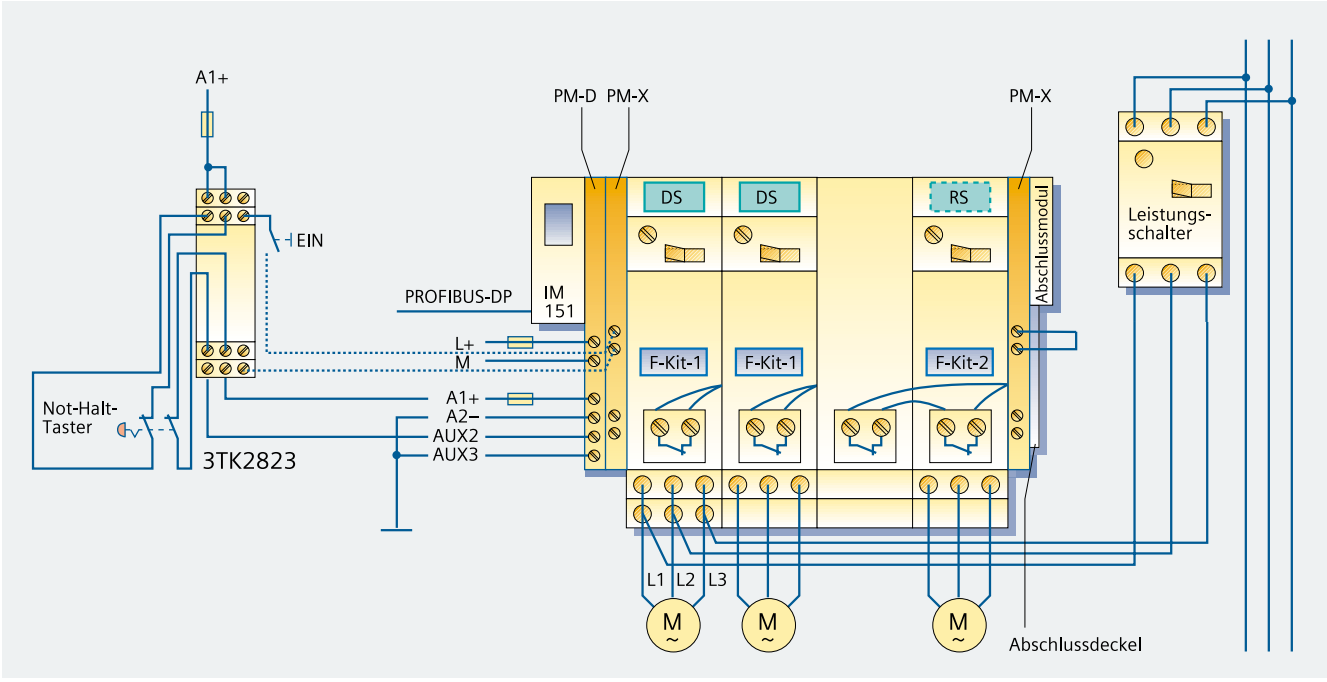


Bild 3/17
ET 200S Motorstarter Solution Local mit externer Not-Halt Überwachung, Kategorie 2 nach EN 954-1

Beschreibung und zusätzliche Info

- Wird der am 3TK2823 zweikanalig angeschlossene Not-Halt-Taster betätigt, werden die Aktoren abgeschaltet. Dies geschieht, indem das 3TK2823 die Versorgungsspannung der Motorstarter über das PMD Modul abschaltet. Die Sicherheit wird hierbei durch das 3TK2823 gewährleistet.
- Die beiden PM-X – Module und die F-Kits werden für die Auswertung und Überwachung des Rückführkreises benötigt.
- Die Auswertung des Rückführkreises wird vom 3TK2823 übernommen.

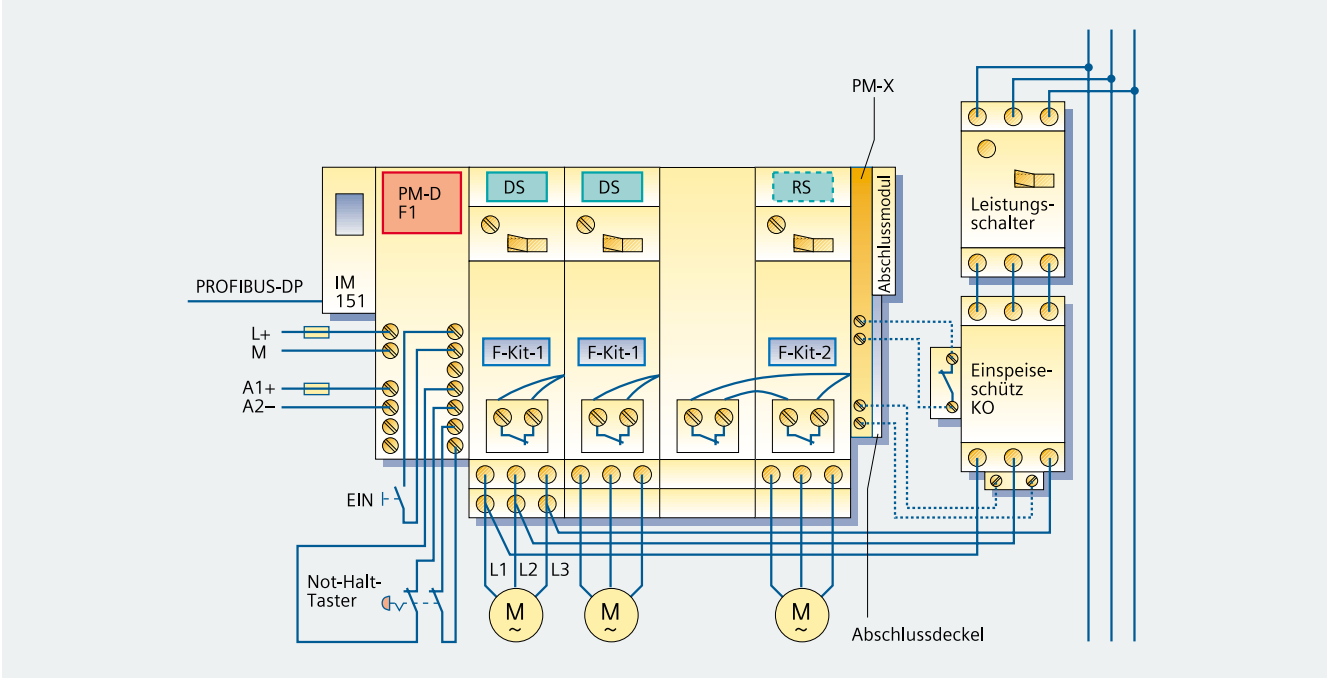


Bild 3/18
ET 200S Motorstarter Solution Local – Not-Halt Überwachung mit überwachtem Start, Kategorie 4 nach EN 954-1

Beschreibung und zusätzliche Info

- Wird der am PM-D F1 zweikanalig verdrahtete Not-Halt-Taster gedrückt, werden die Aktoren abgeschaltet, indem das PM-D F1 die Versorgungsspannung der Motorstarter abschaltet. Der für Kategorie 4 gemäß EN 954-1 erforderliche zweite Abschaltweg wird durch ein zusätzliches Einspeiseschütz realisiert.
- Verzichtet man auf das Wegschalten des Einspeiseschützes, erfüllt diese Applikation Kategorie 2, (siehe hierzu auch Bild 3/17). Mit dem PM-X-Modul und den F-Kits wird der Rückführkreis geschlossen. Das PM-X-Modul stellt außerdem die Klemmen (Ansteuerung und Rücklesekontakt) für das Einspeiseschütz zur Verfügung.
- Die Auswertung des Rückführkreises wird vom PM-D F1 Modul übernommen.

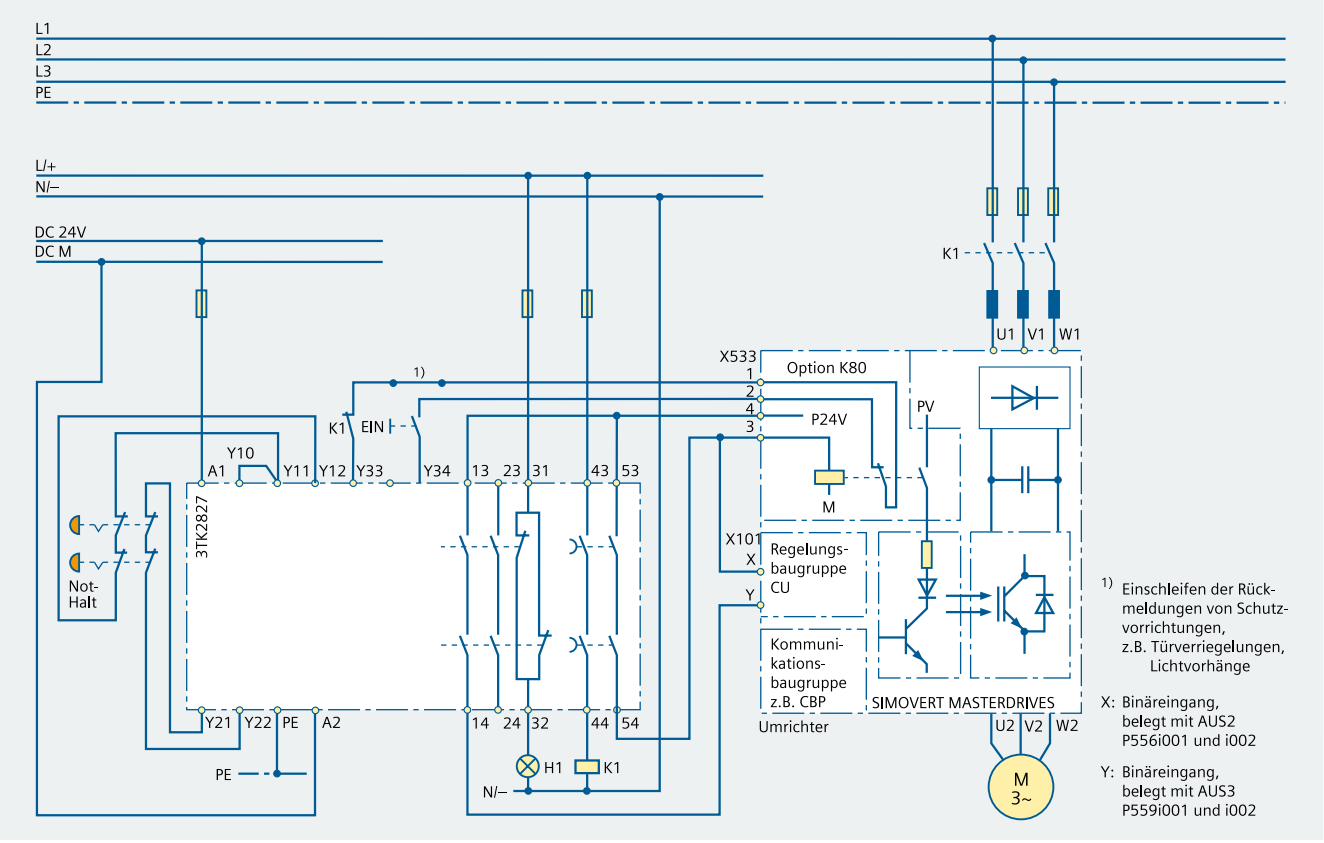


Bild 3/19
SIMOVERT MASTERDRIVES Stop-Kategorie 1, nach EN 60204-1, Kategorie 3 nach EN 954-1; Funktion Sicherer Halt mit geführtem Stillsetzen des Antriebs

Beschreibung und zusätzliche Info

- Mit dieser Lösung wird mit MASTER DRIVES in Verbindung mit einem Sicherheitsschaltgerät die Funktion Sicherer Halt mit geführtem Stillsetzen des Motors an der Momentengrenze realisiert.
- Bei Betätigung des Not-Halt Tasters wird durch den unverzögerten Kontakt der Sicherheitsschaltgerätes am Umrichter ein schnellstmögliches Bremsen des Antriebs eingeleitet.
- Nach Ablauf der an dem Sicherheitsschaltgerät eingestellten Zeit, fallen über die verzögerten Kontakte das Netzschütz und das integrierte Relais des Antriebs ab. Der Antrieb ist zweikanalig gegen ungewollten Wiederanlauf gesichert.
- Sollte durch einen Fehler das Netzschütz oder das integrierte Relais nicht abgefallen sein, wird ein Wiedereinschalten des Sicherheitsschaltgerätes verhindert, der Fehler wird entdeckt (siehe auch Bild 3/47).

Anbindung am AS-Interface mit ASIsafe

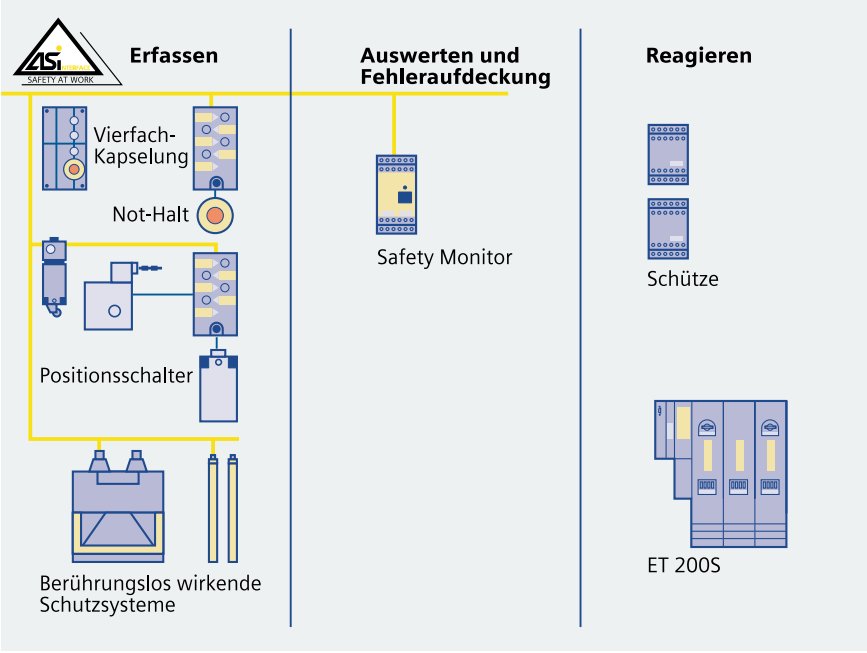


Bild 3/20
Übersicht ASIsafe

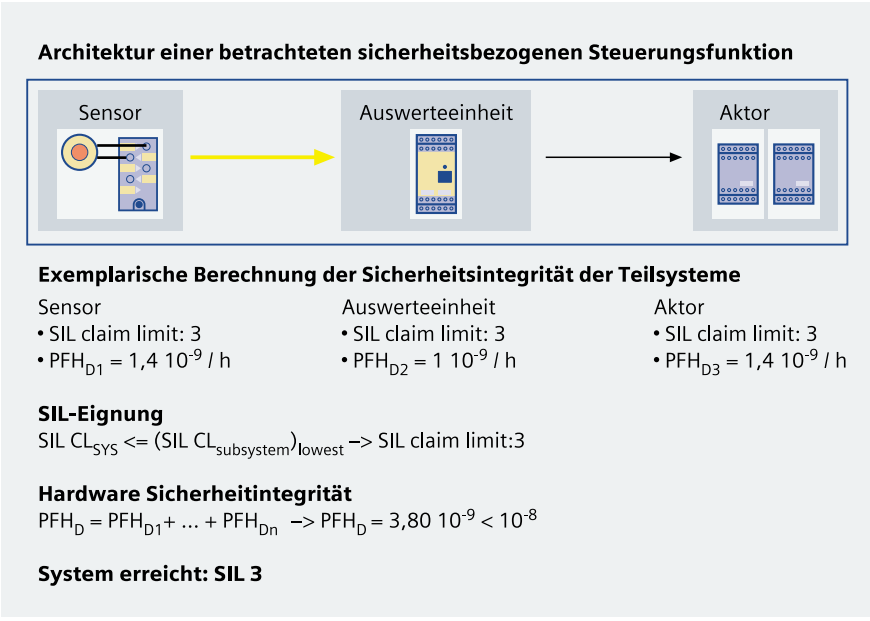

Architektur einer betrachteten sicherheitsbezogenen Steuerungsfunktion
Sensor
Auswerteeinheit
Aktor
Exemplarische Berechnung der Sicherheitsintegrität der Teilsysteme
Sensor
• SIL claim limit: 3
• PFH$_{D1}$ = 1,4 10^{-9} / h
Auswerteeinheit
• SIL claim limit: 3
• PFH$_{D2}$ = 1 10^{-9} / h
Aktor
• SIL claim limit: 3
• PFH$_{D3}$ = 1,4 10^{-9} / h
SIL-Eignung
SIL CL$_{SYS}$ <= (SIL CL$_{subsystem}$)$_{lowest}$ –> SIL claim limit:3
Hardware Sicherheitintegrität
PFH$_D$ = PFH$_{D1}$+ ... + PFH$_{Dn}$ –> PFH$_D$ = 3,80 10^{-9} < 10^{-8}
System erreicht: SIL 3

Bild 3/21
Anwendungsbeispiel für die Anwendung nach der IEC 62061 bei der Anbindung am AS-Interface mit ASIsafe

Die Applikation Bild 3/21 besteht aus folgenden Teilsystemen:

- Erfassen (Not-Halt Taster 2-kanalig)
- Auswerten (ASIsafe Sicherheits-monitor; mit Diagnose)
- Reagieren (zwei Schütze)

Die zur Berechnung heran gezogenen PFH$_D$ Werte sind beispielhaft und keine Originalwerte.

Sensor Anbindung am AS-Interface mit ASIsafe

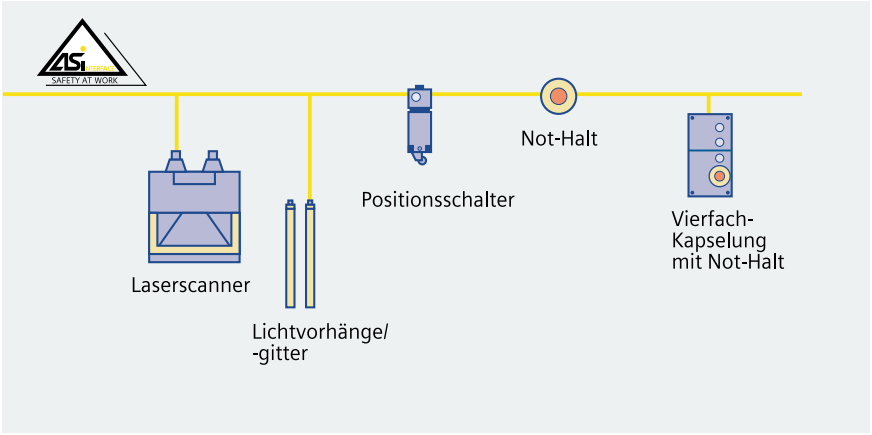


Bild 3/22
Direktanbindung an ASIsafe

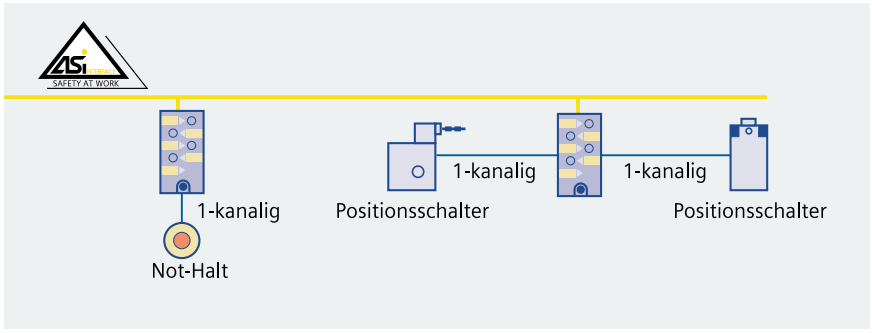


Bild 3/23
Sensor Anbindung über dezentrale Kompaktmodule in Kategorie 2 nach EN 954-1 mit ASIsafe

Beschreibung und zusätzliche Info

- Die Einbindung der Sensoren erfolgt 1-kanalig.
- Je Kompaktmodul können unabhängig voneinander zwei elektromechanische Sensoren nach Kategorie 2 gemäß EN 954-1 angeschlossen werden.
- Wird nur ein 1-kanaliger Sensor angeschlossen (Bild 3/24), müssen die Pins 1 und 2 des nicht angeschlossenen Eingangs gebrückt werden.

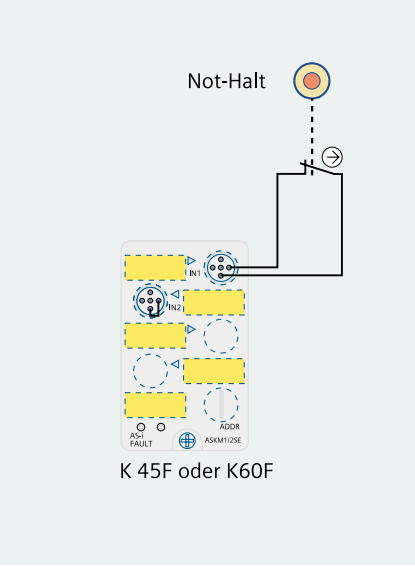


Bild 3/24
Anschluss eines Not-Halt Tasters, Kategorie 2 nach EN 954-1 mit einem sicheren Kompaktmodul

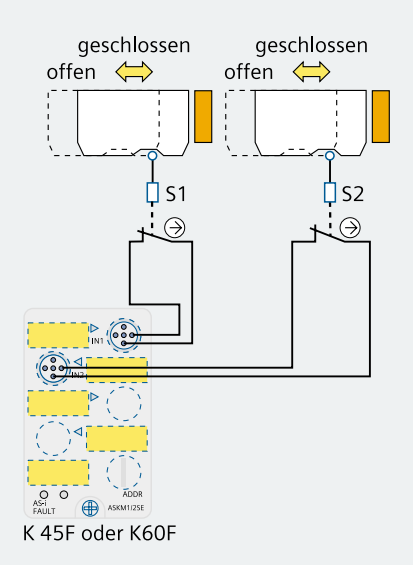


Bild 3/25
Anschluss zweier Schutztürüberwachungen, Kategorie 2 nach EN 954-1 mit einem sicheren Kompaktmodul

Beschreibung und zusätzliche Info

- Mit einem Kompaktmodul können zwei Schutztüren in Kategorie 2 nach EN 954-1 überwacht werden.
  Die Auswertung erfolgt hier unabhängig.

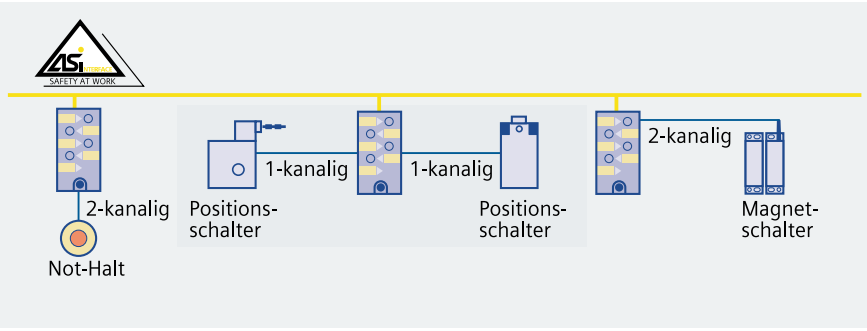


Bild 3/26
Sensor Einbindung über dezentrale sichere Kompaktmodule in Kategorie 4 nach EN 954-1 mit ASIsafe

Beschreibung und zusätzliche Info

- Die Einbindung der Sensoren erfolgt 1-kanalig in abhängiger Auswertung oder 2-kanalig.
- Je Kompaktmodul kann ein 2-kanaliger, elektromechanischer Sensor nach Kategorie 4 gemäß EN 954-1 angeschlossen werden.
- Wird Eingang 2 nicht genutzt, muss dieser mit einer M12 Verschlusskappe verschlossen werden, um IP67 sicherzustellen.

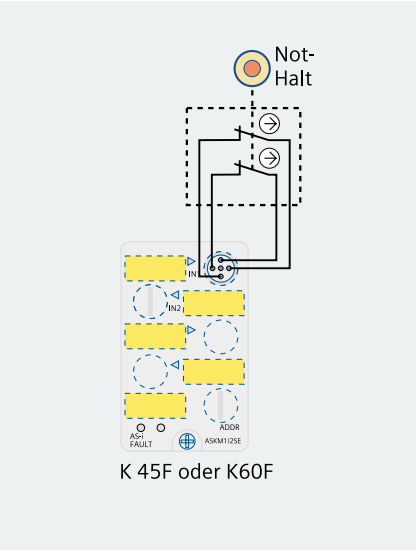


Bild 3/27
Anschluss eines Not-Halt Tasters, Kategorie 4 nach EN 954-1 mit einem sicheren Kompaktmodul

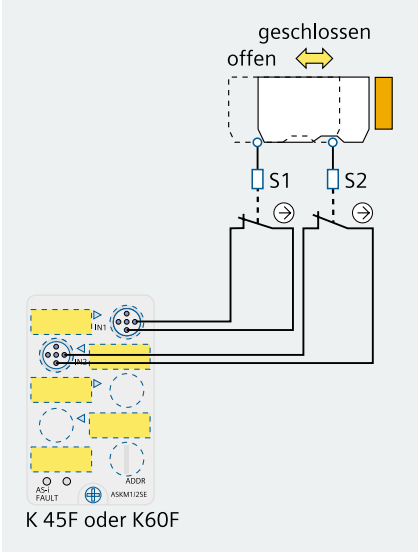


Bild 3/28
Anschluss einer Schutztürüberwachung Kategorie 4 nach EN 954-1 mit einem sicheren Kompaktmodul

Beschreibung und zusätzliche Info

- Mit einem sicheren Kompaktmodul kann eine Schutztür nach Kategorie 4 nach EN 954-1 überwacht werden.

Aktor Anbindung am AS-Interface mit ASIsafe

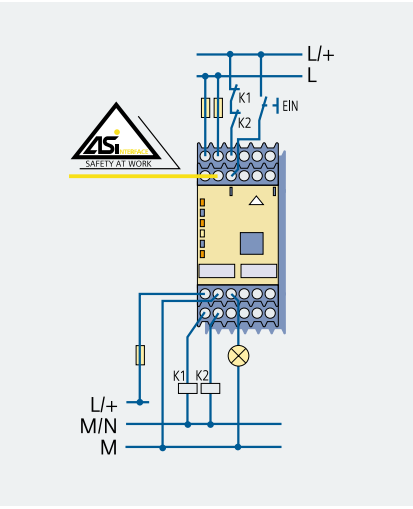


Bild 3/29
Aktor Anbindung Kategorie 4 nach EN 954-1 mit ASIsafe am Beispiel Sicherheitsmonitor mit einem Freigabekreis

Beschreibung und zusätzliche Info

- Der ASIsafe Sicherheitsmonitor wertet alle sicheren Slaves und den Rückführkreis der Schütze (K1, K2) aus.

Die genaue Funktionsweise wird im Kapitel 4.2 beschrieben.

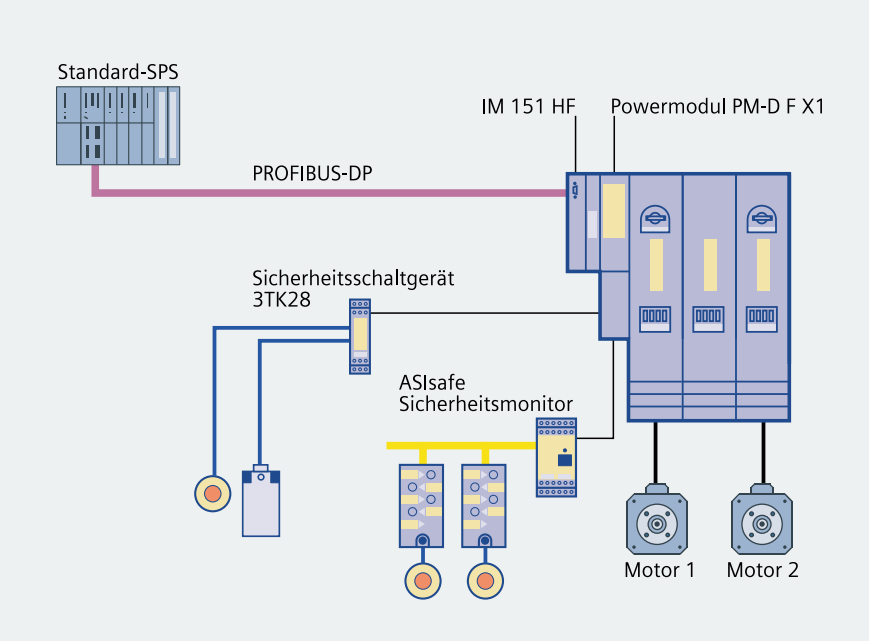


Bild 3/30
ET 200S Motorstarter Solution Local „Abschaltung durch externe Sicherheitssyteme“ in Kategorie 4 nach EN 954-1

Beschreibung und zusätzliche Info

- Die Signale der Sensorik werden über externe sicherheitsgerichtete Auswerteinheiten überwacht, z.B. Sicherheitsschaltgeräte oder ASIsafe.
- Die Freigabekreise der externen sicherheitsgerichteten Auswerte-einheiten werden auf je einen der 6 Sicherheitssegmente verdrahtet, dadurch werden der oder die Failsafe Motorstarter sicherheitsgerichtet abgeschaltet.

Anbindung am PROFIBUS mit PROFIsafe

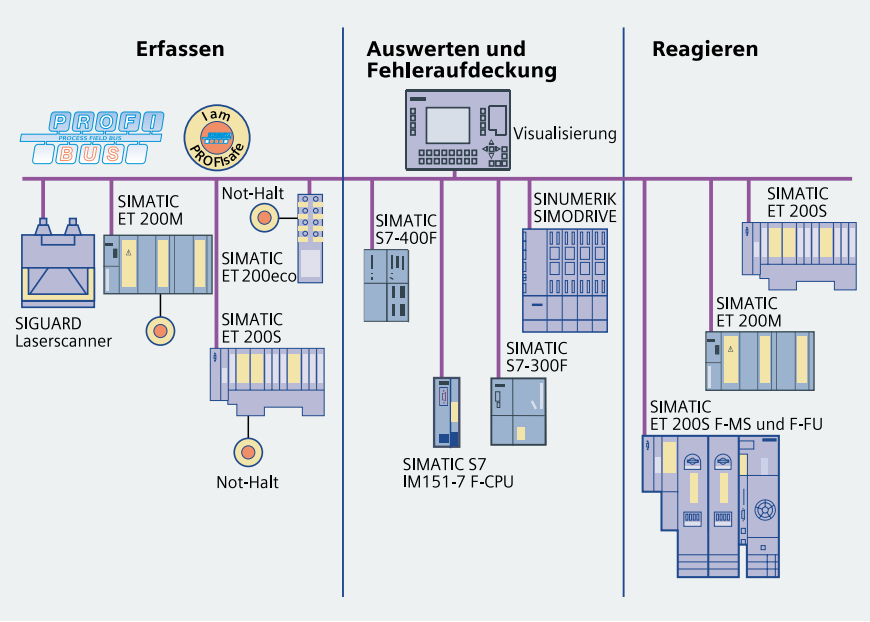


Bild 3/31
Gruppenbild Sensor/Aktor Anbindung am PROFIBUS System

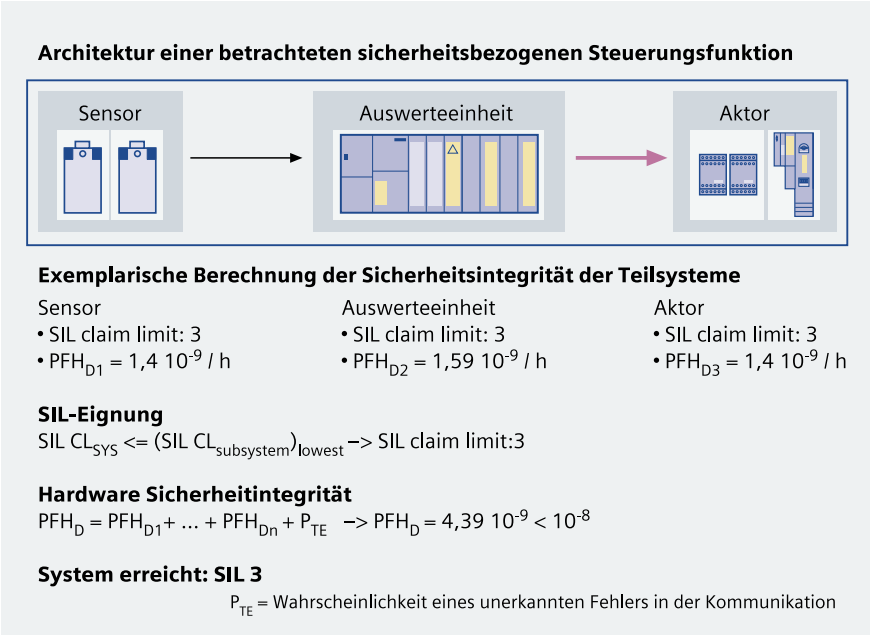

Architektur einer betrachteten sicherheitsbezogenen Steuerungsfunktion
Sensor
Auswerteeinheit
Aktor
Exemplarische Berechnung der Sicherheitsintegrität der Teilsysteme
Sensor
• SIL claim limit: 3
• PFH$_{D1}$ = 1,4 10^{-9} / h
Auswerteeinheit
• SIL claim limit: 3
• PFH$_{D2}$ = 1,59 10^{-9} / h
Aktor
• SIL claim limit: 3
• PFH$_{D3}$ = 1,4 10^{-9} / h
SIL-Eignung
SIL CL$_{SYS}$ <= (SIL CL$_{subsystem}$)$_{lowest}$ –> SIL claim limit:3
Hardware Sicherheitintegrität
PFH$_D$ = PFH$_{D1}$+ ... + PFH$_{Dn}$ + P$_{TE}$ –> PFH$_D$ = 4,39 10^{-9} < 10^{-8}
System erreicht: SIL 3
P$_{TE}$ = Wahrscheinlichkeit eines unerkannten Fehlers in der Kommunikation

Bild 3/32
Anwendungsbeispiel für die Anwendung nach der IEC 62061 bei der Anbindung am PROFIBUS mit PROFsafe

Die Applikation Bild 3/32 besteht aus folgenden drei Teilsystemen:

- Erfassen (zwei Positionsschalter, jeweils 1-kanalig, mit einer ET 200M F-DI Baugruppe, mit Diagnose)
- Auswerten (die F-Steuerung, CPU S7-315F mit Diagnose)
- Reagieren (zwei Schütze, mit einer ET 200M F-DO Baugruppe, mit Diagnose)

Die sicherheitsgerichtete Kommunikation (PROFIsafe) geht als P_{TE} in die Berechnung ein.

Die zur Berechnung heran gezogenen PFH_D Werte sind beispielhaft und keine Originalwerte.

Sensor Anbindung am PROFIBUS mit PROFIsafe

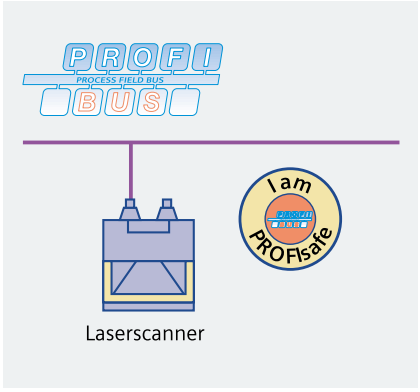


Bild 3/33
Direkte Sensor Anbindung am PROFIBUS

Beschreibung und zusätzliche Info

- Bei der hier dargestellten direkten Sensor Anbindung entfallen zusätzliche Verdrahtungsarbeiten. Jedem Teilnehmer (Slave) wird eine Busadresse zugeordnet.

Sensor Anbindung an fehlersichere SIMATIC Eingabebaugruppen/Module

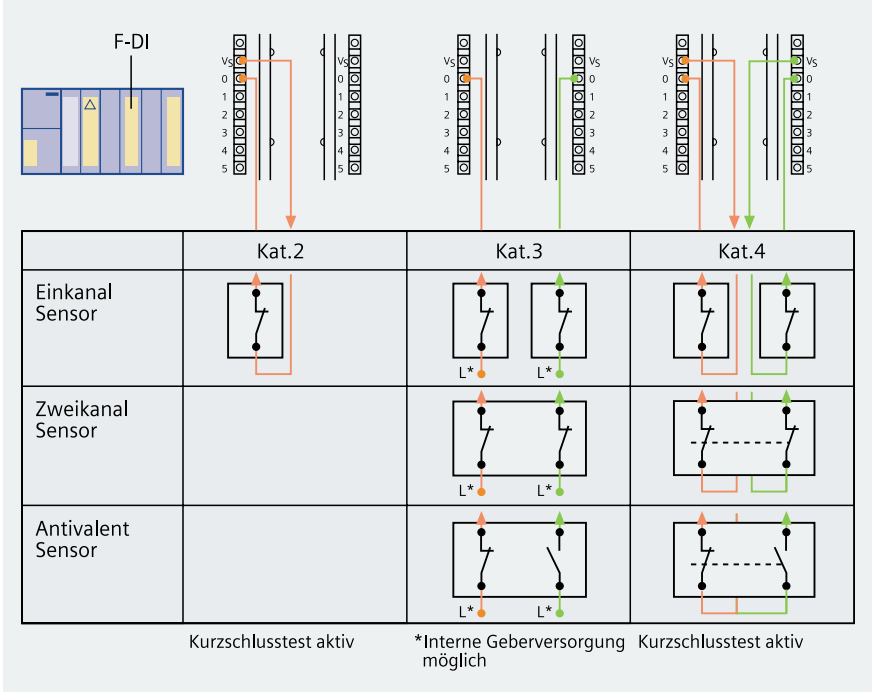


Bild 3/34
Anbindung sicherheitsgerichteter Sensoren. Typischer Anschluss SM326 24DI / ET 200M

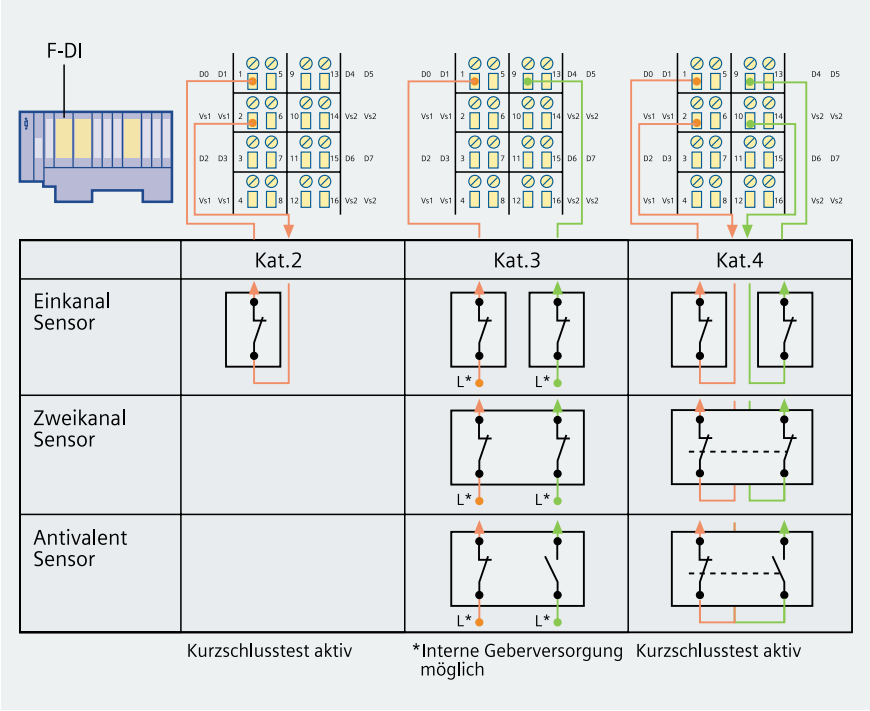


Bild 3/35
Anbindung sicherheitsgerichteter Sensoren. Typischer Anschluss 4/8 F-DI / ET 200S

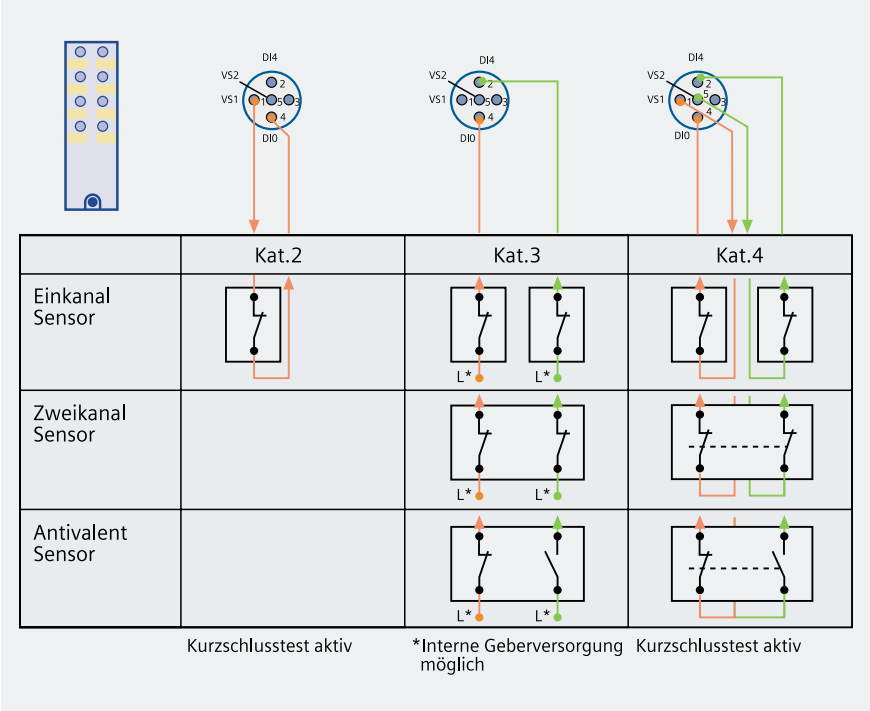
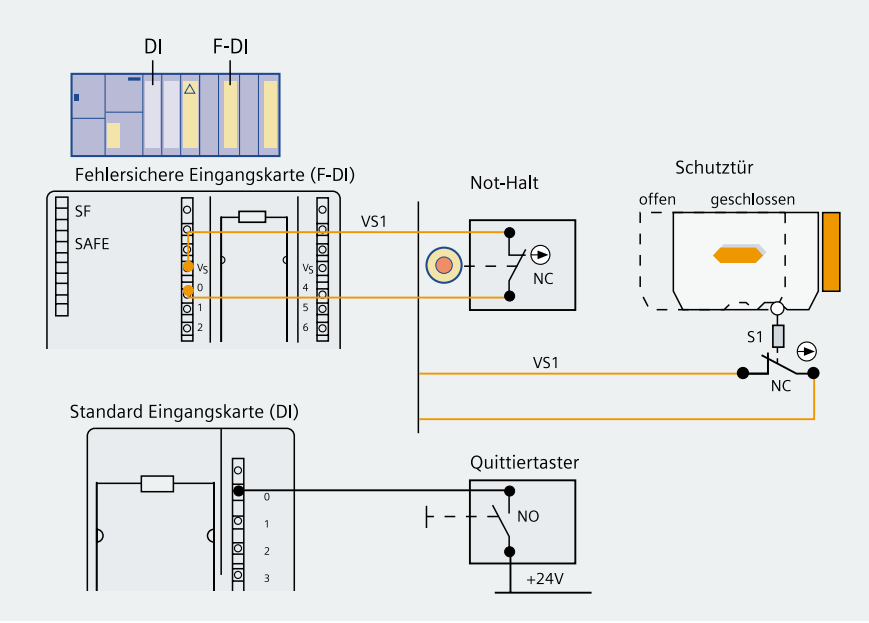


Bild 3/36
Anbindung sicherheitsgerichteter Sensoren. Typischer Anschluss 4/8 F-DI / ET 200eco



Beschreibug und zusätzliche Info

- Die Fehlerüberwachung wird hier von der sicheren F-Eingangsbaugruppe übernommen.
- Die Betätigung der Quittierung darf nicht zum Wideranlauf der Anlage führen.

Bild 3/37
Sensor Einbindung über fehlersichere Eingänge der ET 200M F-Peripherie – am Beispiel Not-Halt, Schutztürüberwachung und Quittierung in Kategorie 2 nach EN 954-1

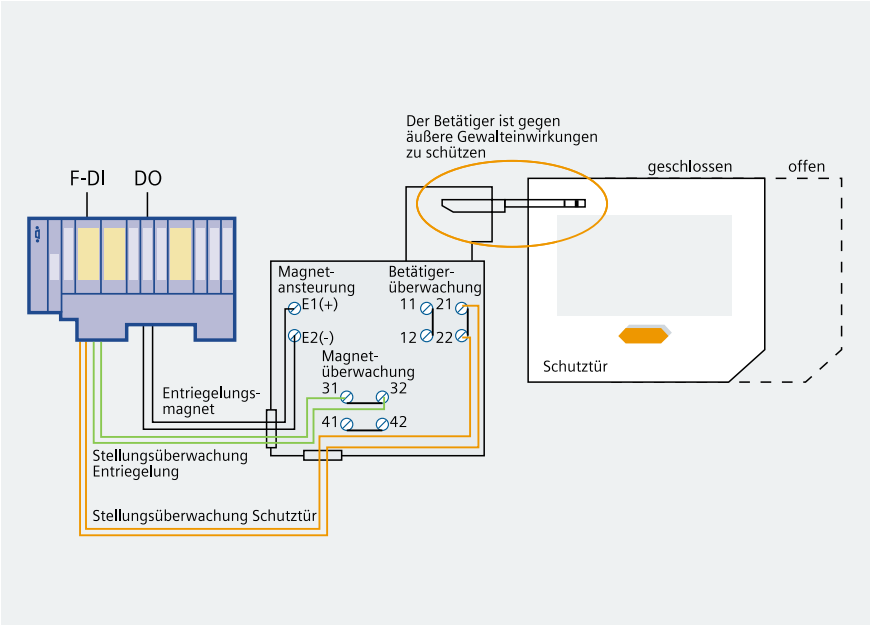


Bild 3/38
Sensor Einbindung über fehlersichere Eingänge der ET 200S F Peripherie – am Beispiel Schutztürüberwachung mit Zuhaltung in Kategorie 3 nach EN 954-1

Beschreibung und zusätzliche Info

Das Besondere an einer Applikation mit einer Schutztür ist die Verkopplung mit weiteren Prozess-Signalen über die "sichere programmierbare Logik". Generell muss die Entriegelung so lange sicher verhindert werden, bis alle Prozessparameter im sicheren Zustand sind. Zum Beispiel darf die Schutztür erst geöffnet werden, wenn

- eine austrudelnde Spindel eine ungefährliche Drehzahl angenommen hat oder stillsteht.
- eine vertikale Achse nach dem Bremsentest mit defekter Bremse in eine sichere Position (Absetz-Position, Absteck-Position) gefahren wurde.
- Aggregate mit gefährlicher Energie im sichern Zustand sind, wie z.B. Laser oder Hydraulik.

Für Kategorie 3 nach EN 954-1 ist bei Verwenden eines einzelnen Positionsschalters der Bruch des Betätigers auszuschließen. Kann der Bruch des Betätigers nicht ausgeschlossen werden, muss ein zweiter Positionsschalter zusätzlich eingesetzt werden (siehe auch Bild 3/42).

Nicht sichere Ansteuerung des Magneten

der Zuhaltung ist bis Kategorie 3 nach EN 954-1 möglich.

Sichere Ansteuerung des Magneten

der Zuhaltung ist ab Kategorie 4 nach EN 954-1 notwendig.

Ziel einer Zuhaltungseinrichtung ist es, eine trennende Schutzeinrichtung in der geschlossenen Position zu halten. Außerdem ist die Schutzeinrichtung mit der Maschinensteuerung verbunden, so dass die Maschine nicht anlaufen kann, wenn die Schutzeinrichtung nicht geschlossen und zugehalten ist, und die trennende Schutzeinrichtung so lange zugehalten bleibt, bis das Verletzungsrisiko aufgehoben ist.

Anmerkung:

Die Ansteuerung der Zuhaltung muss bis Kategorie 3 nach EN 954-1 nicht sicher erfolgen, bei Kategorie 4 nach EN 954-1 muss diese jedoch immer sicher sein. Die Stellungsüberwachung der Verriegelungseinrichtung (Magnet) muss ab Kategorie 3 nach EN 954-1 einzeln erfolgen, nicht in Reihe geschaltet mit der Überwachung des getrennten Betätigers (wegen der sonst mangelnden Fehleraufdeckung).

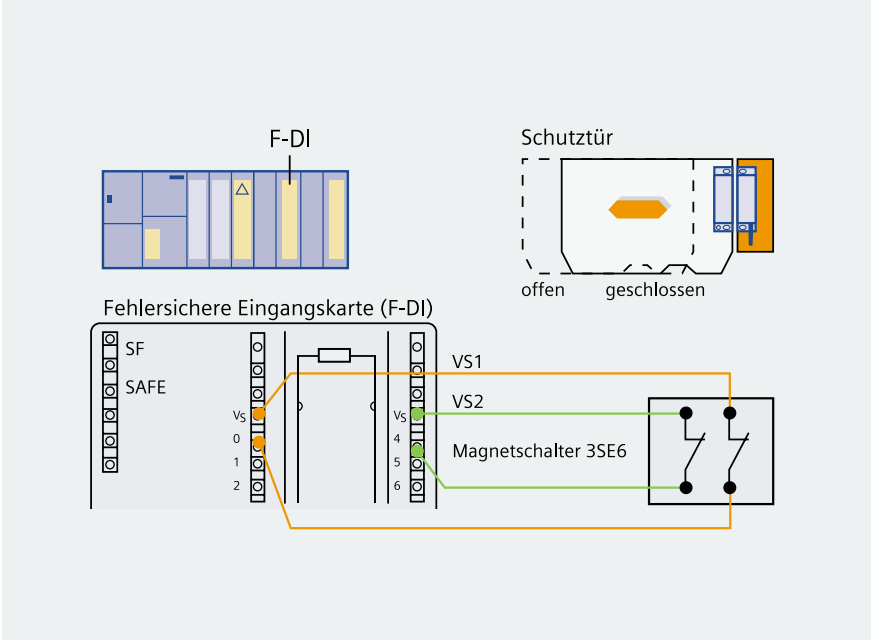


Bild 3/39
Sensor Einbindung über fehlersichere Eingänge der ET 200M F Peripherie – am Beispiel fehlersichere Schutztürüberwachung mit Magnetschalter in Kategorie 4 nach EN 954-1

Beschreibung und zusätzliche Info

- Die berührungslose Schutztürüberwachung besteht aus einem kodierten Magneten und einem Schaltelement (Reed Kontakte).
- Als Spannungsversorgung muss für Kategorie 4 die interne Spannung der fehlersicheren Module verwendet werden. Die Auswertung der Sensoren erfolgt zweikanalig, hierbei muss der Kurzschlusstest in der Baugruppe aktiviert werden.
- An den fehlersicheren Eingängen der SIMATIC S7 300F/400F können auch antivalente Magnetschalter angeschlossen werden.
- Es ist ebenfalls möglich, Magnetschalter am ASIsafe oder an 3TK284x bis Kategorie 4 nach EN954-1 einzusetzen.

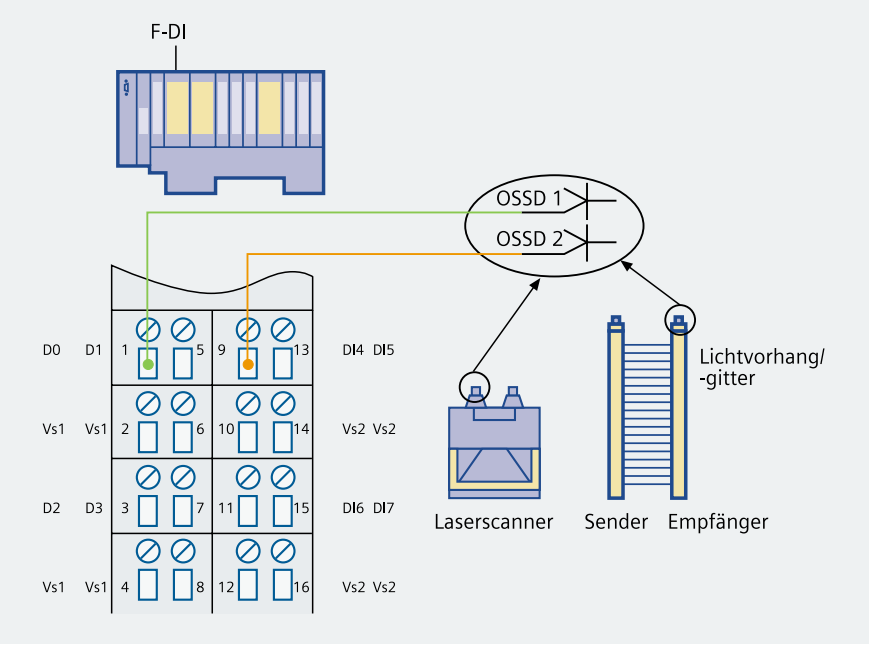


Bild 3/40
Sensor Einbindung über fehlersichere Eingänge der ET 200S F Peripherie – am Beispiel berührungslos wirkender Schutzeinrichtung Typ 3 und 4 nach IEC 61496-1, 2 bzw. EN 61496-1, 2

Beschreibung und zusätzliche Info

- Anstelle des Lichtvorhangs, Lichtgitters bzw. der Lichtschranke kann auch ein Laserscanner direkt angeschlossen werden. (Laserscanner sind bauartbedingt bis Kategorie 3 nach EN 954-1 zugelassen.)
- Auf der fehlersicheren Baugruppe muss die Auswertung zweikanalig erfolgen. Da der notwendige Test auf Kurz- und Querschluss durch die berührungslos wirkende Schutzeinrichtung realisiert wird, muss er in der dazugehörigen Baugruppe abgewählt werden.
- Zusatzfunktionen wie Wiederanlauf und Schützkontrolle, aber auch Taktbetrieb oder Muting, lassen sich durch die Auswertegeräte 3RG7847.. oder wie hier dargestellt mit einer sicherheitsgerichteten Steuerung wie z.B. SIMATIC S7-300F/400F realisieren.

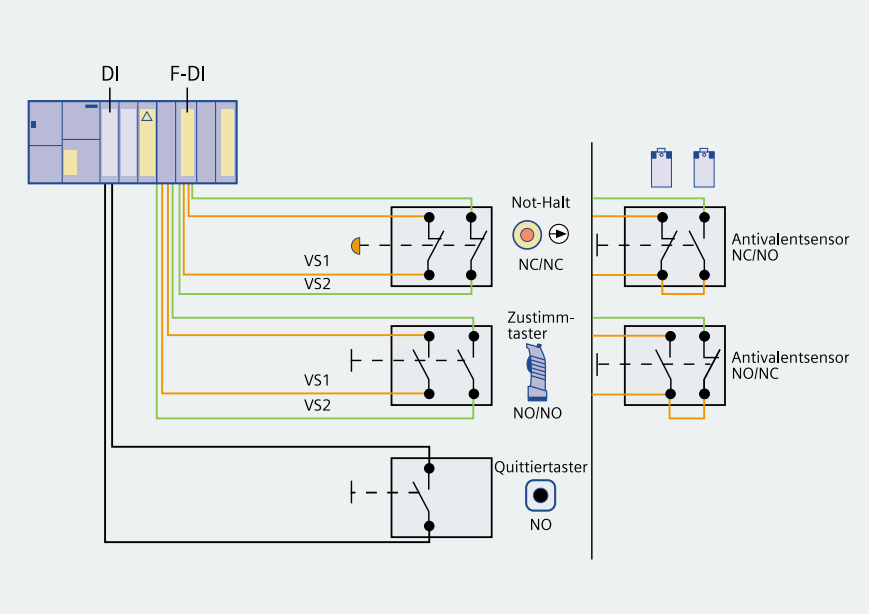


Bild 3/41
Sensor Einbindung über fehlersichere Eingänge der ET 200M F Peripherie – am Beispiel Not-Halt, Zustimmtaster und Quittierung in Kategorie 4 nach EN 954-1

Beschreibung und zusätzliche Info

- Die Quittierung des Not-Halts wird einkanalig auf eine Standard Baugruppe aufgelegt und im Sicherheitsprogramm über eine Flanke ausgewertet.

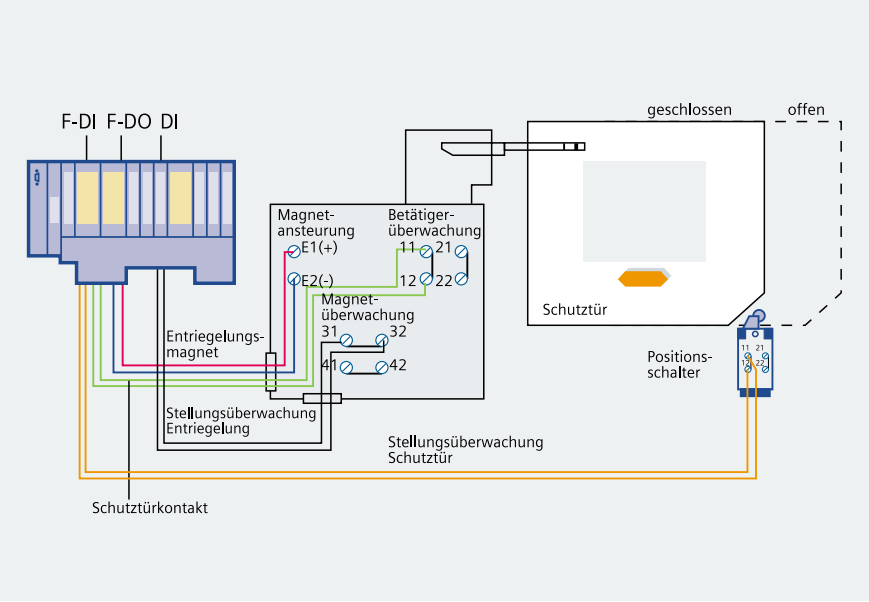


Bild 3/42
Sensor Einbindung über fehlersichere Eingänge der ET 200S F Peripherie – am Beispiel Schutztürüberwachung mit Zuhaltung in Kategorie 4 nach EN 954-1

Beschreibung und zusätzliche Info

- Die Anschaltung für Kategorie 4 nach EN 954-1 unterscheidet sich zu Kategorie 3 (Bild 3/38) durch den zweiten Positionsschalter und der sicheren Anschaltung des Magneten.
- Es ist ebenfalls möglich, Türzuhaltungsschalter am ASIsafe oder an Sicherheitsschaltgeräten 3TK284x bis Kategorie 4 nach EN 954-1 einzusetzen.

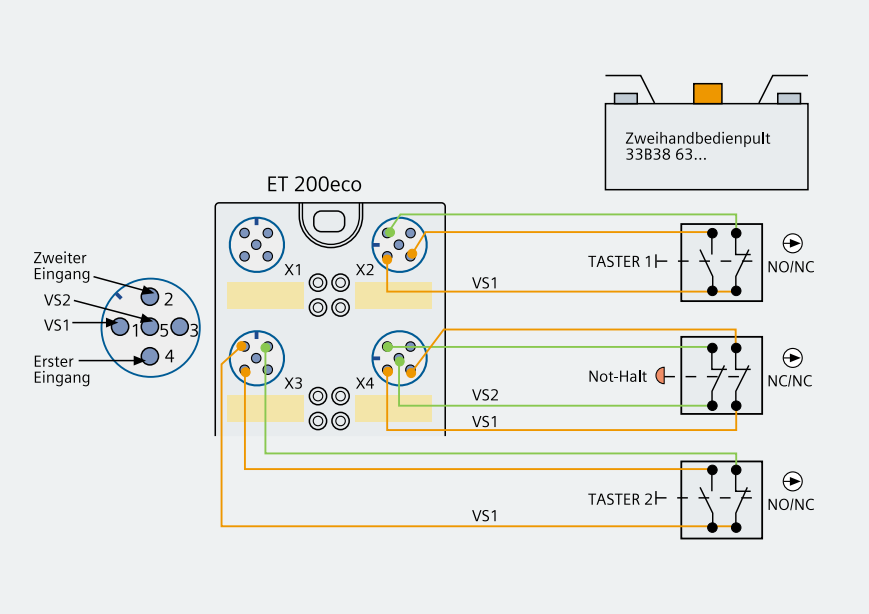


Bild 3/43
Sensor Einbindung über fehlersichere Eingänge der ET 200eco F Peripherie – am Beispiel Zweihandbedienpult Kategorie 4 nach EN 954-1

Beschreibung und zusätzliche Info

- Als Spannungsversorgung muss für Kategorie 4 die interne Spannung der fehlersicheren Module verwendet werden. Die Auswertung der Sensoren erfolgt zweikanalig, hierbei muss der Kurzschlusstest in der Baugruppe aktiviert werden.
- Die Diskrepanzzeit zwischen dem betätigen beider Taster ist gemäß EN 574 einzustellen.
- Ein Zweihandbedienpult kann auch direkt am ASIsafe oder am Sicherheitsschaltgerät 3TK284x bis Kategorie 4 nach EN 954-1 eingesetzt werden.

Aktor Anbindung am PROFIBUS mit PROFIsafe

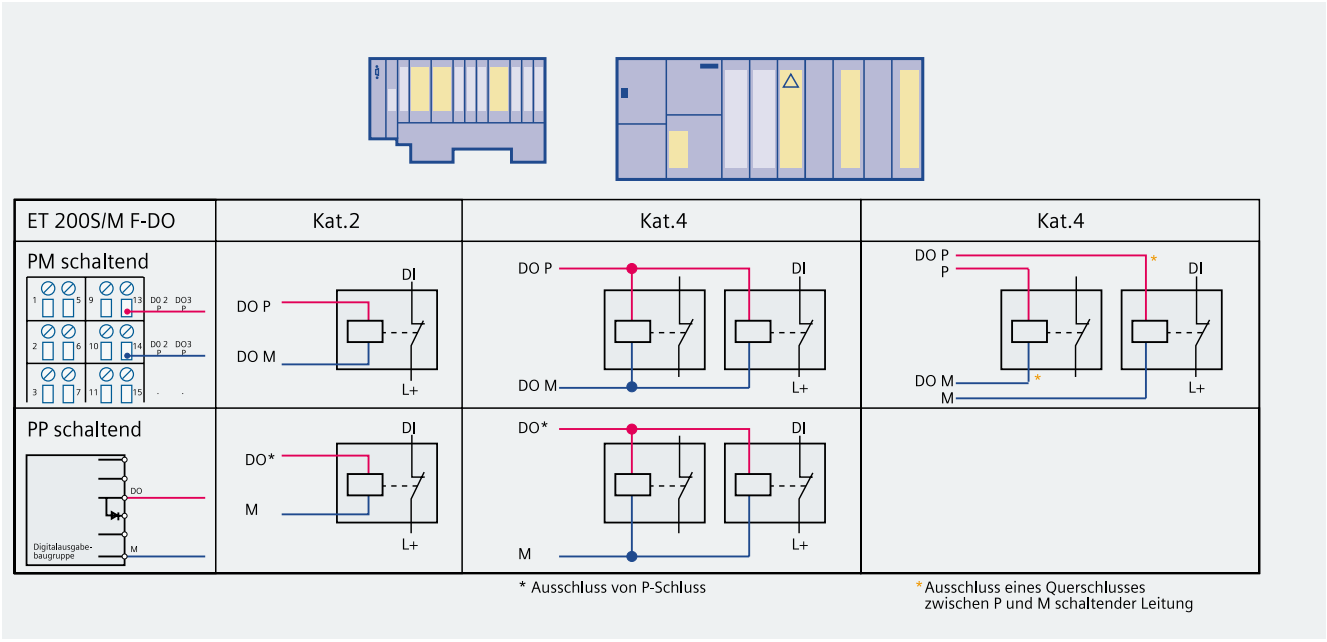


Bild 3/44
Anbindung sicherheitsgerichteter Aktoren Plus-Minus /Plus-Plus schaltend

Rückmeldung vom Lastkreis

- Die Rückmeldung vom Lastkreis ist so direkt wie möglich von der Prozessgröße abzuleiten. Dies geschieht z.B. bei Schützen durch das Rücklesen eines zwangsgeführten Öffnerkontakts. Das Rücklesen muss nicht sicherheitsgerichtet sein!

- Auch ist die direkte Rückmeldung des Hydraulikdruckes über einen Druck-Sensor oder die Rückmeldung der bewegten Mechanik (Endanschlag) über einen Bero, der indirekten Rückmeldung des Hydraulikventils vorzuziehen.

- Die F-DO überwacht die Ansteuerleitungen des Aktors – bei einem Fehler werden die Ausgänge in den sicheren Zustand geschaltet.

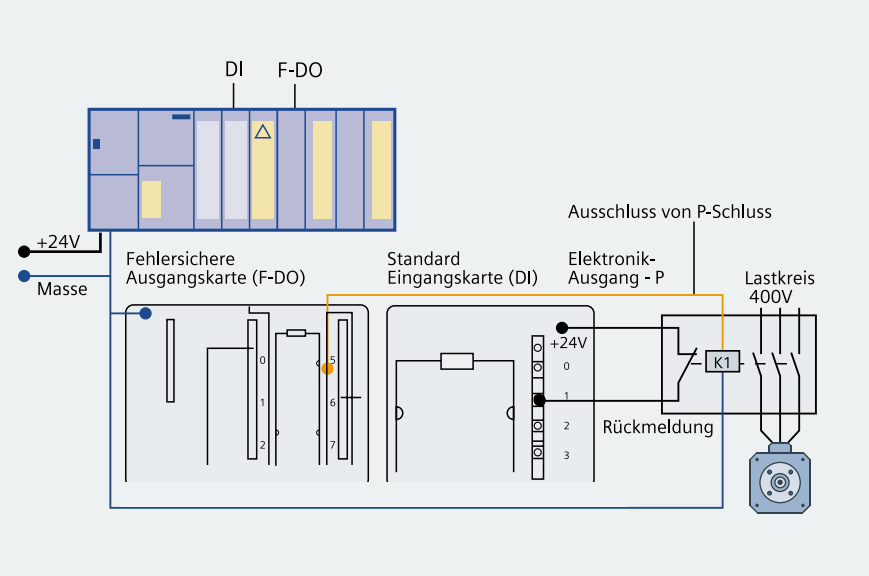


Bild 3/45
Aktor Abschaltung über fehlersichere Ausgänge der ET 200M F-Peripherie in Kategorie 2 nach EN 954-1

Beschreibung und zusätzliche Info

- Bild 3/45 zeigt eine Aktor Abschaltung mit einem ET 200M F-Ausgang. Die erforderliche Rückmeldung des Schützes wird einkanalig über den zwangsgeführten Kontakt auf einen Standard Eingang einer Digitaleingabebaugruppe eingelesen und dynamisch (zeitlich) im fehlersicheren Programm überwacht.

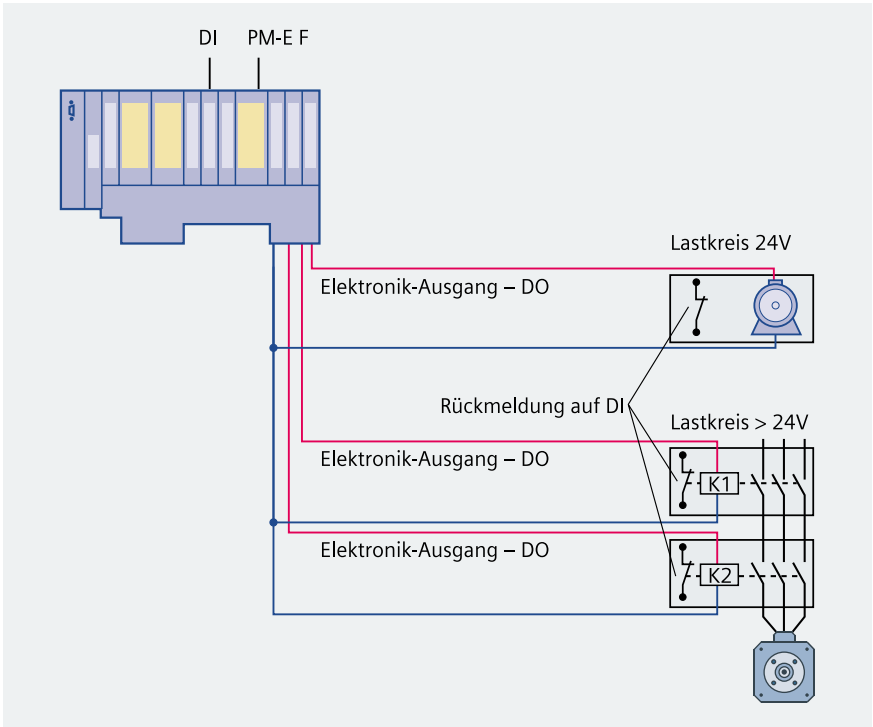


Bild 3/46
Aktor Abschaltung über Standardausgänge der ET 200S F-Peripherie – am Beispiel Gruppenabschaltung Kategorie 3 nach EN 954-1

Beschreibung und zusätzliche Info

- Das betriebsmäßige Schalten erfolgt über Standard-Ausgänge, die nach dem PM-E F Modul gesteckt sind.
- Das PM-E F Modul versorgt die folgenden Standard Baugruppen mit Spannung.
- Im Not-Halt Fall werden die Schütze sicher über das PM-E F Modul abgeschaltet, indem dieses Modul die Versorgungsspannung (P und M) für die Standard-Ausgänge trennt.
- Es dürfen nur zulässige Standardbaugruppen nach der PM-E F für eine sicherheitsgerichtete Abschaltung verwendet werden.

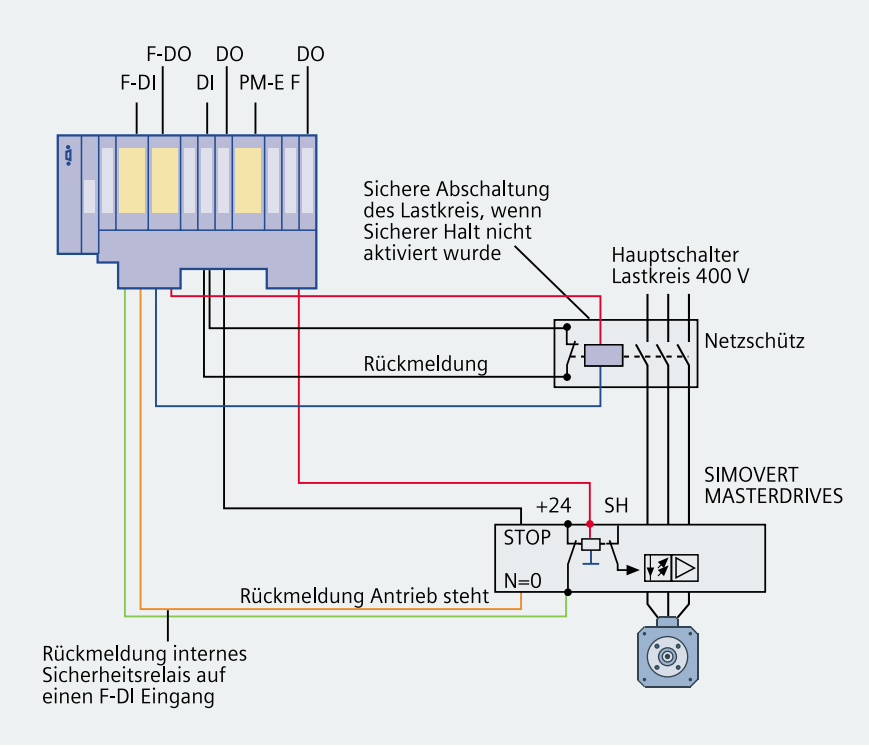


Bild 3/47
Aktor Abschaltung über Standardausgänge der ET 200S F-Peripherie – am Beispiel SIMOVERT MASTERDRIVES Stop-Kategorie 1, nach EN 60204-1, in Kategorie 3 nach EN 954-1; Funktion Sicherer Halt mit geführtem Stillsetzen des Antriebs

Beschreibung und zusätzliche Info

- Sicherer Halt:
  Die Funktion Sicherer Halt (SH) verhindert den unerwarteten Anlauf des angeschlossen Motors aus dem Stillstand. Sicherer Halt soll erst nach Stillstand des Antriebes aktiviert werden, da er andernfalls seine Fähigkeit zum Bremsen verliert.

- Über einen Eingang des Frequenzumrichters (STOP) wird der Antrieb so schnell wie möglich abgebremst. Nach dessen Stillstand oder spätestens nach einer festgelegten maximalen Überwachungszeit wird der Sichere Halt aktiviert.

- Die zwangsgeführten Rückmeldekontakte des im Frequenzumrichter integrierten Relais müssen in der F-Steuerung dahingehend ausgewertet werden, dass eine Fehlfunktion des Relais (z.B. verklebte Kontakte) erkannt und dann das übergeordnete Netzschütz abgeschaltet wird.

- STOP und Sicherer Halt wird über eine Standard Ausgabebaugruppe nach dem PM-E-F angesprochen.
  Im fehlersicheren Programmteil wird die Stromschiene des PM-E-F abgeschaltet, sobald der Sichere Halt aktiviert wurde (Siehe auch Bild 3/19).

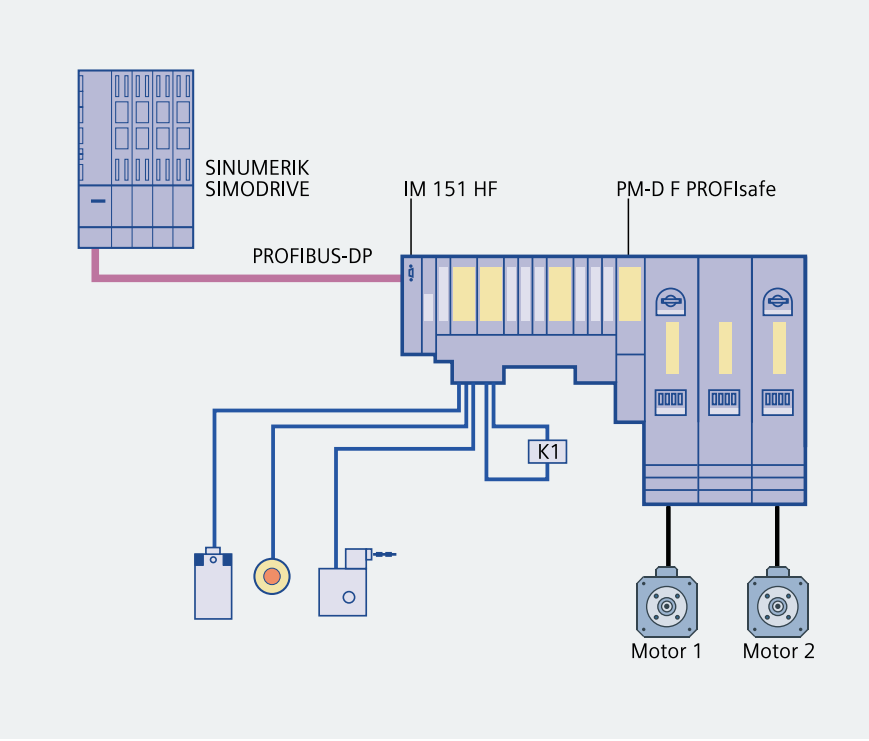


Bild 3/48
Aktor Abschaltung – am Beispiel der ET 200S F-Peripherie in Kategorie 3 nach EN 954-1 an der SINUMERIK 840D PROFIsafe

Beschreibung und zusätzliche Info

- Die Sensoren und Aktoren werden, je nach erforderlicher Kategorie, einkanalig oder zweikanalig an die fehlersichere Peripherie der ET 200S angeschlossen und über PROFIsafe an den SINUMERIK Master weitergegeben.
- Der SINUMERIK Master schaltet bedarfsabhängig die Motorstarter über das PM-D F PROFIsafe, sowie die fehlersicheren Ausgänge direkt ab.

Mit diesem Beispiel wird Kategorie 3 nach EN 954-1 erreicht werden, da der SINUMERIK Master nach Kategorie 3 zertifiziert ist.

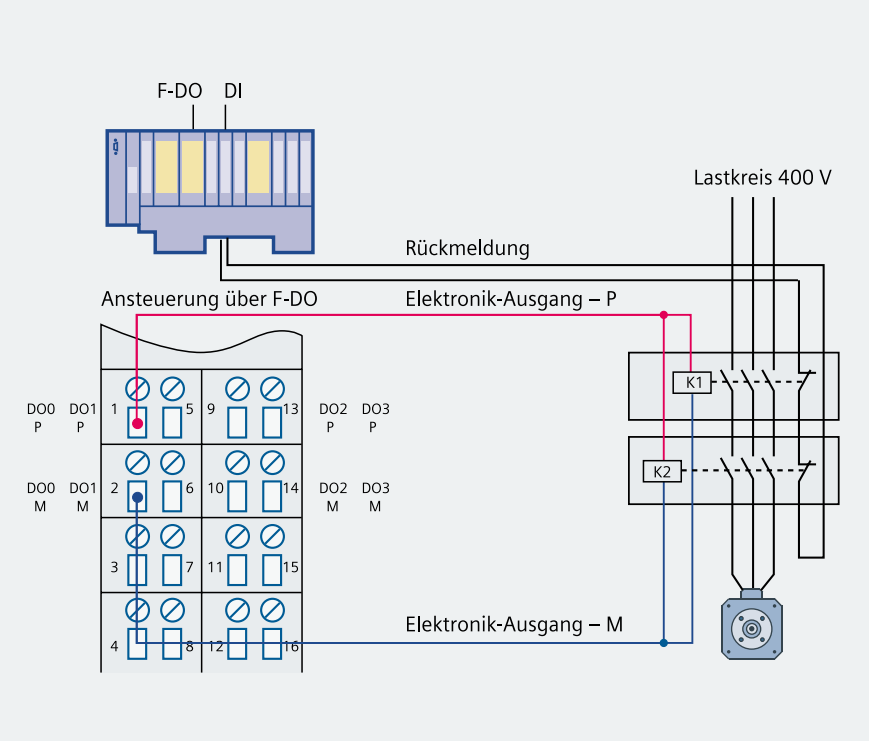


Bild 3/49
Aktor Abschaltung über fehlersichere Ausgänge der ET 200S F-Peripherie – am Beispiel Aktor Abschaltung Kategorie 4 nach EN 954-1

Beschreibung und zusätzliche Info

- Das Beispiel Bild 3/49 zeigt eine Aktor Abschaltung mit nur einem ET 200S F-Ausgang.
- Die erforderliche Rückmeldung der Schütze wird einkanalig über die zwangsgeführten Kontakte auf den Standardeingang einer digitalen Eingabebaugruppe eingelesen und dynamisch (zeitlich) im fehlersicheren Programm überwacht.

Varianten

- Ein Motorstarter der ET 200S PROFIsafe ersetzt die diskrete Schaltung über zwei Lastschütze (siehe Bild 3/50).

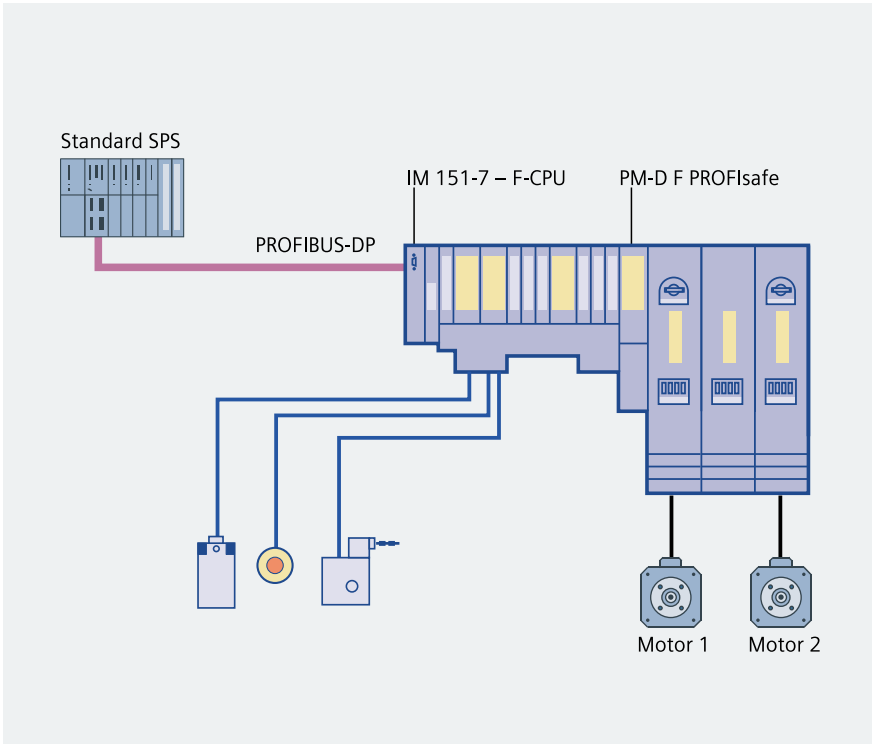


Bild 3/50
Aktor Abschaltung über eine „lokale Sicherheitsinsel“ – am Beispiel der IM 151-7 F-CPU in Kategorie 4 nach EN 954-1

Beschreibung und zusätzliche Infos

- In dem Beispiel wird die Sensorik dezentral in einer ET200S Station überwacht.
- Die F-CPU (IM 151-7 F-CPU) schaltet je nach Bedarf sicher die Motorstarter ab. Dies geschieht, indem das PM-D F PROFIsafe einen Abschaltbefehl erhält und eine oder mehrere Sicherheitsgruppen (Safety Groups) wegschaltet, auf denen die Motorstarter hardwareseitig kontaktiert und softwareseitig parametriert sind.

Varianten

- Wird die Sensorik dezentral z.B. mit ASIsafe eingelesen und über den ASIsafe Monitor überwacht, kann man mit den sicheren Ausgängen des Monitors direkt die Sicherheitsgruppen (Safety Groups) mit Zuhilfenahme eines PM-D F-X1 Moduls selektiv schalten. Hierfür ist keine F-CPU erforderliche (siehe Bild 3/30).

4.1 PROFIsafe
4.2 ASIsafe

Fehlersichere Kommunikation

über Standard-Feldbusse

4

4 Fehlersichere Kommunikation über Standard-Feldbusse

Fehlersichere Kommunikation über Standard-Feldbusse mit PROFIsafe und ASIsafe

Die Forderungen nach weiteren Einsparungspotenzialen in der Automatisierungstechnik können vor allem durch die Wahl der richtigen Installationstechnik erfüllt werden. In der Standardtechnik führte die konsequente Umsetzung der Dezentralisierung mit der Nutzung von modernen Feldbustechnologien bereits zu erheblichen Kosteneinsparungen. Weitere Einsparmöglichkeiten ergeben sich in Zukunft durch die zusätzliche Übertragung der sicherheitsrelevanten Signale über den bereits verlegten Standard-Feldbus.

Gesamtsystem mit integrierter Sicherheit

Durch das Aufsetzen der sicherheitsgerichteten Kommunikation auf diese bewährten Standard-Feldbusse sind Anlagenprojekteure in der Lage, sowohl in der Standardtechnik als auch in der Sicherheitstechnik mit den gleichen Engineering-Werkzeugen und -Methoden wirtschaftlicher zu arbeiten. Im Gegensatz zu Konzepten einer sicheren Datenübertragung über Spezialbusse ergibt sich hier eine optimale Datentransparenz zwischen dem Standard- und dem Sicherheitsteil einer Gesamtanlage, ohne zusätzliche Schnittstellen.

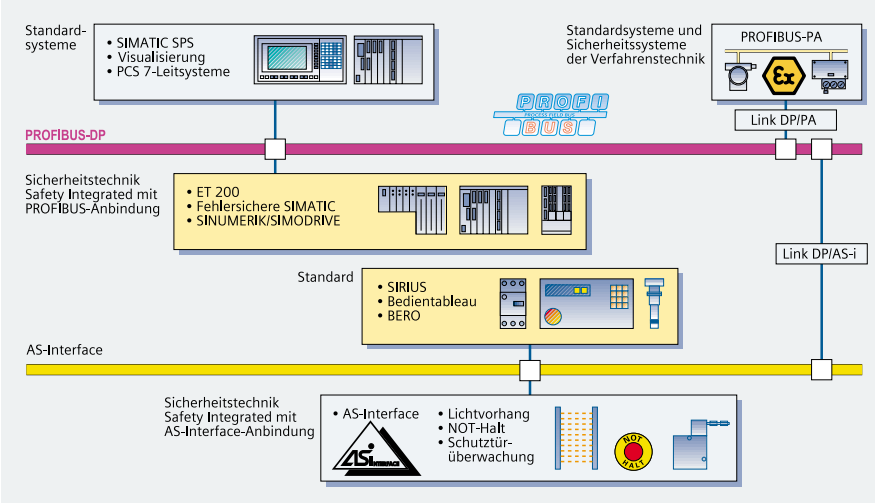


Bild 4/1
Das Grundprinzip von „Safety Integrated“: ein durchgängiges Automatisierungssystem mit integrierten Sicherheitsfunktionen

4.1 PROFIsafe

Koexistenz von PROFIsafe und PROFIBUS-Teilnehmern am gleichen Kabel

Die hauptsächliche Vorgabe bei der Definition des PROFIsafe-Profils war die rückwirkungsfreie Koexistenz der

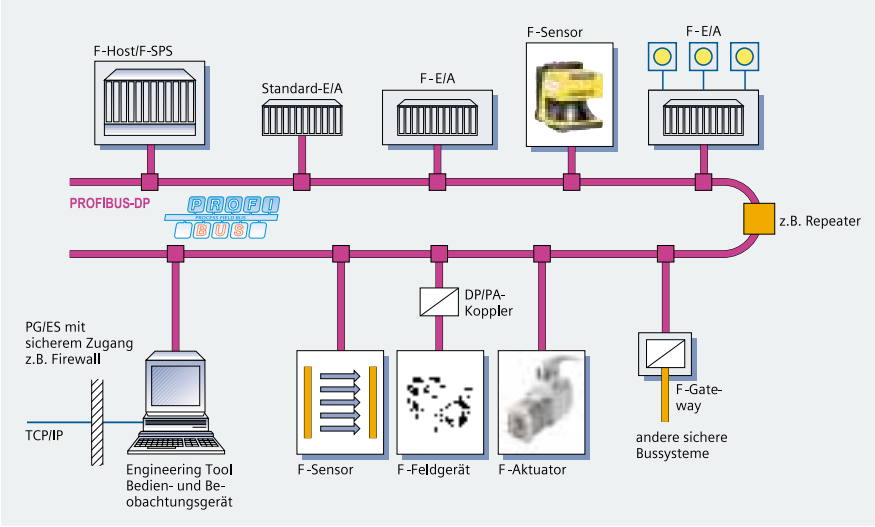


Bild 4/2
Koexistenz von PROFIsafe- und PROFIBUS-Teilnehmern am gleichen Kabel

sicherheitsgerichteten und der Standardkommunikation auf ein und demselben Buskabel. Weiterhin sollte die erforderliche Sicherheit auf einem 1-kanaligen Kommunikationssystem möglich sein, jedoch der optionale Weg zu erhöhter Verfügbarkeit, durch Redundanz der Nachrichtenkanäle, nicht verbaut werden.

Mit PROFIsafe sicher kommunizieren über PROFIBUS-DP

Die PROFIBUS-Nutzerorganisation (PNO) hat bereits im Frühjahr 1999, als Ergebnis eines Arbeitskreises, Richtlinien für die sichere Kommunikation auf dem Standard-PROFIBUS unter dem geschützten Markennamen PROFIsafe veröffentlicht, die von BIA und TÜV durch positive technische Berichte bestätigt wurden.

Ziel des Arbeitskreises war es von Anfang an, möglichst viele Partner an der Definition und der Lösungsfindung zu beteiligen und die Ergebnisse in einer offenen Weise zur Verfügung zu stellen. So waren, neben Herstellern von Sicherheitssystemen, mehr als 25 namhafte nationale und internationale Hersteller von sicheren Sensoren und Aktoren, Werkzeugmaschinenfabriken, Endanwender und Universitätsinstitute vertreten. Zwischen- und Endergebnisse wurden ständig mit dem TÜV und dem BIA abgestimmt. Bedeutende Beiträge kamen vom Verein Deutscher Werkzeugmaschinenfirmen (VDW). Über die gemeinsame Durchsprache von Sicherheitsszenarien ist so quasi ein „normiertes" vollständiges Anforderungsprofil für dezentrale Sicherheitstechnik entstanden, an dem das PROFIsafe-Konzept stets gespiegelt werden konnte.

Außerdem bestand die Anforderung, auch komplexere Geräte der optischen Sicherheitstechnik, z.B. Laserscanner und Lichtvorhänge, einzubinden.

Merkmale/Nutzen

Die folgenden Abschnitte zeigen, wie PROFIsafe all die genannten Anforderungen erfüllt.

Freizügige Realisierung sicherheitsgerichteter Anlagen

Mit PROFIsafe können sicherheitsgerichtete Anlagen sehr flexibel realisiert werden. Einerseits ist eine Ein-Kabel-Lösung mit einer kombinierten Standard- und Sicherheitsautomatisierung in einer CPU möglich. Andererseits können dafür aber auch zwei CPUs und zwei getrennte Buskabel verwendet werden. Die „homogene Lösung" mit einem einzigen Bussystem bietet natürlich Vorteile – insbesondere hinsichtlich des Engineerings.

Technische Vorteile von PROFIsafe

PROFIsafe setzt auf den eingeführten Standard-Kommunikationskomponenten wie Kabeln, ASICs und Softwarepaketen auf. Die Sicherheitsmaßnahmen sind in den sicherheitsgerichteten Kommunikationsendteilnehmern gekapselt. Grundsätzlich bestehen keine Einschränkungen hinsichtlich Baudrate, Zahl der Busteilnehmer oder der Übertragungstechnik, sofern die geforderten Reaktionszeiten der Automatisierungsaufgabe dies jeweils zulassen. Außerdem hat PROFIsafe den Vorteil, dass der Anwender hinsichtlich Buskabel, Schirmung, Buskoppler usw. keine besondere Maßnahmen treffen muss.

Alle bei der Kommunikation auftretenden Fehler werden durch das PROFIsafe-Protokoll abgefangen. Dazu stellt PROFIsafe sicher, dass in den Telegrammen die Werte korrekt übertragen und dass die Telegramme in einer definierten Zeit eintreffen. Außerdem

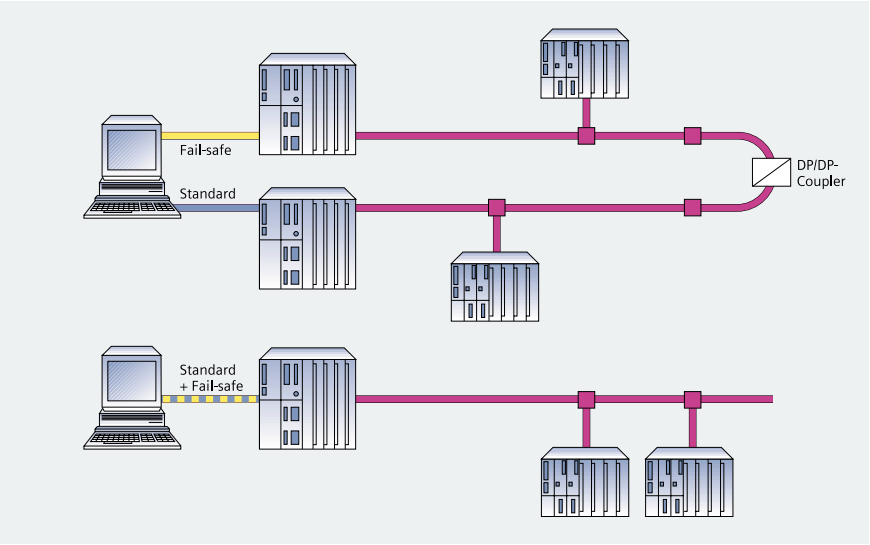


Bild 4/3
Varianten für sicherheitsgerichtete Anlagen (unten: ein Bussystem für Standard- und Sicherheitsautomatisierung, oben: Standard- und Fail-safe-Bussystem getrennt aufgebaut)

ermöglicht PROFIsafe auch den Anschluss sicherheitsgerichteter komplexer Endgeräte, die eine umfangreichere Parametrierung erfordern oder komplexe Daten liefern können.

Einsatzbereiche von PROFIsafe

PROFIsafe kommt immer dann zum Einsatz, wenn bei verteilten Anlagen Sicherheit in der Kommunikation über PROFIBUS erforderlich ist. Das ist insbesondere dann der Fall, wenn an einen vorhandenen Bus zusätzlich sichere Teilnehmer angeschlossen werden sollen, ohne dadurch aufwändige Hardware-Erweiterungen vornehmen zu müssen.

Die PROFIsafe-fähigen Produkte

Als erstes PROFIsafe-Produkt weltweit wurden 1999 die SIMATIC S7-414FH und S7-417FH (siehe Kapitel 7) mit dezentraler fehlersicherer Peripherie ET 200M eingeführt. Sie können auch redundant aufgebaut werden und garantieren zusätzlich Hochverfügbarkeit – sind also besonders für die Prozessautomatisierung prädestiniert. Außerdem stehen mit der SIMATIC S7-315F, S7-317F und S7-416F (siehe Kapitel 7) weitere fehlersichere SPSen mit dem Schwerpunkt Fertigungstechnik zur Verfügung. Neben der ET 200M erweitern die ET 200S und ET 200eco das fehlersichere Peripheriespektrum.

Hinzu kommen komplexe Sensoren und Aktoren und berührungslos wirkende Schutzeinrichtungen (BWS) aus dem SIGUARD Safety Integrated Programm mit Direktanschluss an PROFIBUS/PROFIsafe. In gleicher Weise lässt sich auch die fehlersichere SINUMERIK 840D anbinden.

Welche Sicherheitsstufen erreicht PROFIsafe?

Die Entwicklung der PROFIsafe-Richtlinie wurde bereits nach der Norm IEC 61508 durchgeführt. Pate stand die prEN 50159-1, die für den Bahnbereich ähnliche Lösungswege aufzeigte. Weitere relevante Normen und Standards wurden berücksichtigt. Die erreichten Sicherheitsstufen sind Safety Integrity Level 3 (IEC 61508), Kat. 4 (EN 954-1).

PROFIsafe im 7-Schichten-Kommunikationsmodell

Die Sicherheitsmaßnahmen beim PROFIsafe-Profil befinden sich über der Schicht 7 des ISO/OSI-Kommunikationsmodells. Hierzu bedarf es einer weiteren Schicht, die sich sicherheitsgerichtet um die Beschaffung und Aufbereitung der Nutzdaten kümmert. In einem sicheren Feldgerät kann diese Funktion z.B. durch dessen Technologie-Firmware wahrgenommen werden.

Wie im Standardbetrieb auch, werden die Prozesssignale bzw. Prozesswerte in entsprechende Nutztelegramme verpackt. Sie werden bei sicheren Daten lediglich um Sicherungsinformationen ergänzt.

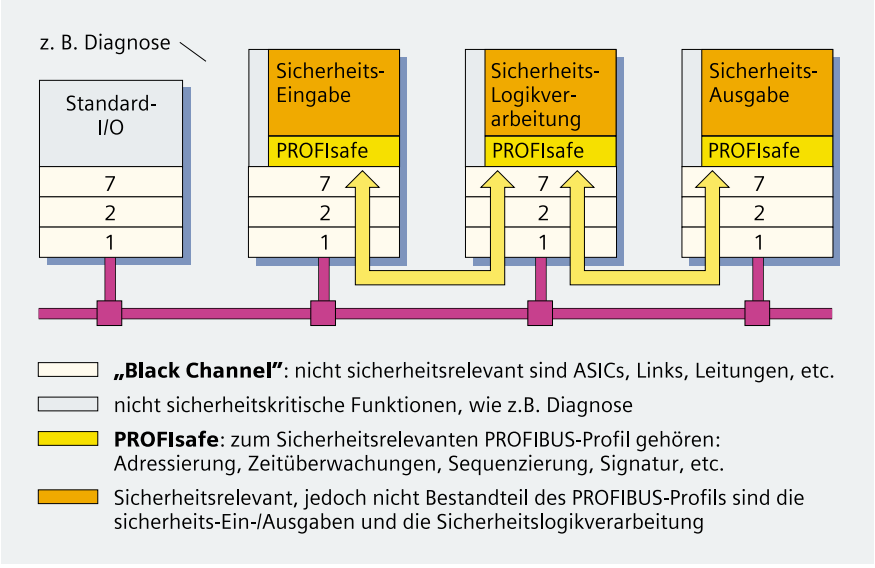


Bild 4/4
PROFIsafe Safety-Layer oberhalb des OSI-Modells

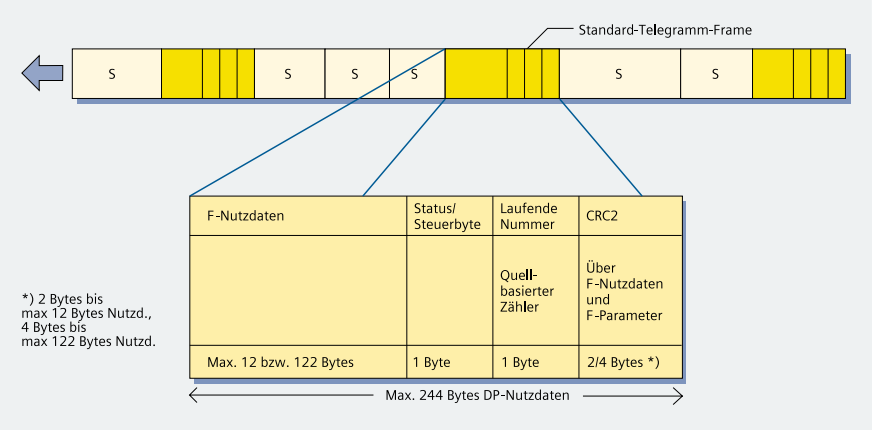


Bild 4/5
PROFIsafe-Telegramme einfach in Standardtelegramme verpackt

Für den Versand der sicherheitsgerichteten Telegramme wird ebenfalls ein Standardmechanismus „Master-Slave-Betrieb" von PROFIBUS genutzt. Ein Master, der in der Regel einer CPU zugeordnet ist, tauscht zyklisch mit allen seinen konfigurierten Slaves Telegramme aus.

PROFIsafe-Funktionen

PROFIsafe ermöglicht einerseits die sichere Kommunikation durch Beherrschung sämtlicher Kommunikationsfehler; dabei wird laufend die Sicherheit am PROFIBUS überwacht. Andererseits lässt PROFIsafe auch die Anbindung komplexer Endgeräte durch entsprechende Protokoll-Erweiterungen zu.

Mögliche Kommunikationsfehler

Beim Versand von Telegrammen können eine Reihe von Fehlern auftreten. Telegramme können verloren gehen, wiederholt auftreten, zusätzlich eingefügt werden, in falscher Reihenfolge oder verzögert auftauchen und Daten verfälschungen aufweisen. Hinzu kommt noch fehlerhafte Adressierung, das heißt, ein Standard-Telegramm erscheint irrtümlich bei einem Sicherheitsteilnehmer und gibt sich als Sicherheitstelegramm aus (Maskerade).

PROFIsafe-Mechanismen für sichere Kommunikation

In Bild 4/6 sind die möglichen Fehlerursachen und die bei PROFIsafe gewählten Abhilfemaßnahmen in eine Matrix eingetragen. Zu diesen zählen

- die fortlaufende Nummerierung der Sicherheitstelegramme,
- eine Zeiterwartung mit Quittierung,
- eine Kennung für Sender und Empfänger („Losungswort") und
- eine zusätzliche Datensicherung (CRC – cyclic redundancy check).

Anhand der fortlaufenden Nummer kann ein Empfänger erkennen, ob er sämtliche Telegramme in der korrekten Reihenfolge empfangen hat.

Maßnahme: / Fehler:	Laufende Nummer (Lebenszeichen)	Zeiterwartung mit Quittierung	Kennung für Sender und Empfänger	Datensicherung
Wiederholung	x			
Verlust	x	x		
Einfügung	x	x	x	
Falsche Abfolge	x			
Verfälschung von Nutzdaten				x
Verzögerung		x		
Kopplung von sicherheitsrelevanten und Standard-Nachrichten (Maskerade), einschließlich Falsch- und Doppeladressierung		x	x	x
FIFO Fehler innerhalb des Routers		x		

Bild 4/6
Mögliche Kommunikationsfehler und PROFIsafe-Maßnahmen zur Aufdeckung

In der Sicherheitstechnik kommt es nicht allein darauf an, dass ein Telegramm die richtigen Prozesssignale oder Werte überträgt, sondern diese müssen auch innerhalb einer definierten Zeit (Fehlertoleranzzeit) eintreffen, so dass der jeweilige Teilnehmer gegebenenfalls Sicherheitsreaktionen automatisch vor Ort einleiten kann. Hierzu verfügen die Teilnehmer über eine einstellbare Zeitüberwachung (Time-out), die nach dem Eintreffen eines Sicherheitstelegramms neu „aufgezogen" wird.

Die 1:1-Beziehung zwischen Master und einem Slave erleichtert die Erkennung von fehlgeleiteten Telegrammen. Beide müssen lediglich über eine im Netzwerk eindeutige Kennung ("Losungswort") verfügen, an Hand derer sie die Authentizität eines Telegramms überprüfen können. Eine Schlüsselrolle spielt die Datensicherung über CRC. Ihr kommt zusätzlich die Verantwortung zu, neben der Datenintegrität der transportierten Nutzdaten auch die Integrität der im jeweiligen Endgerät deponierten Parameter sicherzustellen.

Da die Datensicherungsmaßnahmen und die Zuverlässigkeit des Standard-PROFIBUS für den Sicherheitsnachweis nicht herangezogen wurden, war dieser Sicherheitsnachweis für PROFIsafe zwar etwas aufwändiger, hat aber den Vorteil, dass der Anwender hinsichtlich Buskabel, Schirmung, Buskoppler usw. für PROFIsafe keine besondere Maßnahme treffen muss.

SIL-Monitor zur Sicherheitsüberwachung am PROFIBUS

In der prEN 50159-1 ist ein Markov-Modell angegeben, welches in geringfügig erweiterter Form für die Berechnung der Restfehlerwahrscheinlichkeiten von Sicherheitskreisen eingesetzt werden konnte. Es geht von drei wesentlichen Einflüssen für die Verfälschung von Nachrichten aus, die allesamt von den beiden Datensicherungseinrichtungen erkannt werden müssen: Ausfälle in ASICs und Treibern, elektromagnetische Störungen und der spezielle Fall, dass lediglich die Sicherungseinrichtung im Bus-ASIC ausgefallen ist. Ohne besondere Maßnahmen hätte sonst für jede Buskonfiguration ein gesonderter Nachweis erbracht werden müssen.

Für einen offenen Standard-Feldbus wie den PROFIBUS wäre dies eine gravierende Einschränkung.

Es wurde daher eine Einrichtung geschaffen, die die Einhaltung von SIL-Stufen über die Lebenszeit einer dezentralen sicheren Automatisierungslösung, unabhängig von den eingesetzten Komponenten und der Konfiguration, gewährleistet: ein patentierter SIL-Monitor. Der SIL-Monitor ist in Software realisiert. Er berücksichtigt alle vorstellbaren Fehlereinflüsse und löst eine Reaktion aus, wenn die Anzahl der Störungen oder Fehler ein bestimmtes Maß pro Zeiteinheit übersteigt. Die Zahl der zulässigen Fehler pro Zeiteinheit ist abhängig von der eingestellten SIL-Stufe.

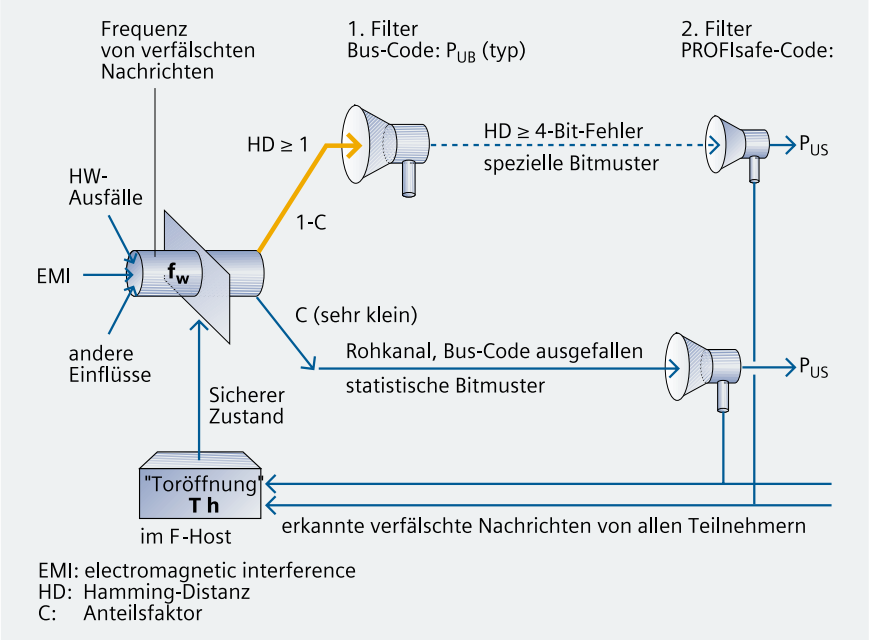


Bild 4/7
Patentierter SIL-Monitor überwacht laufend die funktionale Sicherheit des PROFIsafe

Anschluss von komplexen Endgeräten an PROFIsafe

Über die Szenariendurchsprache war den Arbeitskreis-Mitgliedern schnell klar geworden, dass eine reine Profilbeschreibung für die schnelle Umsetzung in eine Vielzahl von „PROFIsafe-Produkten" nicht ausreichen würde. Insbesondere die optische Sicherheitstechnik, mit z.B. Laserscannern und Lichtvorhängen, benötigt große Mengen von Parametern, deren Einlernphasen eine spezielle Bedienung erfordern. Hierfür hat der Arbeitskreis in den Richtlinien Lösungen beschrieben, die auch für weitere komplexe Geräte angewandt werden können. Parametrierung und Diagnose von PROFIsafe-Komponenten können – wie bei PROFIBUS üblich – über einen direkt am PROFIBUS angeschlossenen PC erfolgen.

Um das Projektieren von Sicherheitskreisen optimal zu vereinfachen, stehen den Engineering-Tools alle notwendigen Parameter zur Verfügung. Insbesondere für die Berechnung von Gesamtreaktionszeiten der Sicherheitskette müssen von den Herstellern in den GSD (Gerätestammdaten)-Datenblättern die Bearbeitungszeiten von Sensoren und Aktuatoren angegeben werden.

PROFIsafe im Zusammenspiel mit TIA

Damit bietet PROFIsafe für die Sicherheitstechnik einen ähnlich hohen Grad an Integration und Durchgängigkeit wie die Standard-Automatisierung am PROFIBUS. Dies ist ganz im Sinne von „Totally Integrated Automation" (TIA) und schafft Freiräume zur Lösung von noch anspruchsvolleren Aufgaben.

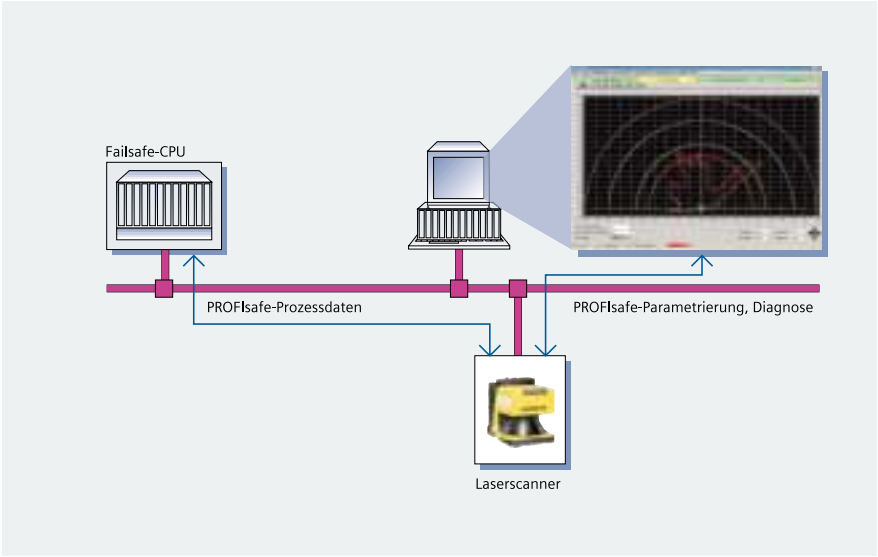


Bild 4/8
Parametrierung und Diagnose von PROFIsafe-Komponenten

4.2 ASIsafe

Das System am AS-Interface

Übersicht

Das Konzept AS-Interface Safety (im folgenden kurz „ASIsafe") ermöglicht die Integration von sicherheitsgerichteten Komponenten wie Not-Halt-Schalter, Schutztür-Schalter oder Sicherheits-Lichtgitter direkt an einem AS-Interface Netz zum fehlersicheren Schutz für Mensch, Maschine und Umwelt.

Mit ASIsafe kann bis Kategorie 4 (EN 954-1) bzw. SIL3 (IEC 61508) sicherheitsgerichtet abgeschalten werden, ohne die Vorteile der einfachen und kostengünstigen Verdrahtung zu verlieren.

Durch ASIsafe ergeben sich folgende Vorteile für den Maschinen- und Anlagenbauer:

- Einfache Integration von sicherheitstechnischen Komponenten in die Standard-Automatisierung
- Kostengünstiger Aufbau, da keine fehlersichere SPS bzw. kein spezieller Master benötigt wird
- Schneller Aufbau der Sicherheitstechnik durch flexible Verdrahtung mittels AS-Interface
- Integrierte Diagnose durch AS-Interface erhöht die Wartungsfreundlichkeit des Systems und ermöglicht eine schnelle Fehlerbehebung. Dadurch werden Stillstandszeiten erheblich reduziert.

Die einfache Projektierung und Inbetriebnahme von AS-Interface wird somit auch für die Sicherheitstechnik ermöglicht.

Kundennutzen

- Schneller Aufbau der Sicherheitstechnik durch höchstflexible Topologie und einfache Anschlusstechnik von AS-Interface.
- Minimale Wartungs- und Stillstandszeiten durch integrierte Diagnose.
- Besonders kostengünstiger Aufbau möglich, ohne fehlersicherer SPS und ohne speziellem Master.
- Sichere und nicht-sichere Daten auf einem Bus ermöglichen durchgängige Automatisierungslösung.
- Einfachste Projektierung des AS-Interface mittels eines Knopfdrucks am Master.
- Höchste Sicherheit: Zugelassen bis Kategorie 4 gemäß EN 954-1 und SIL3 gemäß IEC 61508.
- Einfache Projektierung der Sicherheitstechnik durch einfache, graphische Software („asimon").
- Bestehende Systeme können einfach erweitert werden.
- TÜV-Zertifiziert und UL-Approbiert

Vorteile

Vorteile gegenüber konventioneller Sicherheitstechnik:

- Kürzere Stillstandszeiten aufgrund integrierter Diagnose.
- Höhere Flexibilität durch Programmierung statt Verdrahtung der Sicherheitslogik.
- Wesentlich vereinfachte Montage, da beispielsweise komplizierte Rückführverdrahtungen bei verteilten Abschaltungen entfallen.
- Einfaches Duplizieren einer Lösung auf mehrere Maschinen / Anlagen durch Kopieren des Sicherheits-Programms.
- Einfache Modifizierung der Sicherheitslogik durch Programmänderungen.
- Nur eine Schnittstelle zum HMI-System, dadurch durchgängige Diagnose.
- Reduzierte Aufbauzeiten und Kosten durch integrierte Diagnose: Der Zustand der Sicherheitstechnik muss nicht über gesonderte E/A-Baugruppen zur Meldung an die Steuerung geführt werden.
- Reduzierte Ersatzteilhaltung, da die als Anwender Software programmierte Sicherheitslogik unterschiedlichste Hardware ersetzt.
- Schneller Überblick über Sicherheitsfunktionalität der Anlage über ein einfaches graphisches Tool. Komplexe Schaltungsanalysen bei Anlagenerweiterungen entfallen dadurch.
- Sind durch TÜV-Abnahmen zusätzliche Sicherheitsmassnahmen gefordert, so ermöglicht die flexible Verdrahtung und Projektierung ein einfaches Einbinden zusätzlicher Sicherheitskomponenten.

Vorteile gegenüber anderen Sicherheitsfeldbussen:

- Es wird keine fehlersichere SPS und keine spezieller Master benötigt
- Einfaches ungeschirmtes 2-Draht-Kabel beschleunigt und erleichtert den Aufbau
- Durch die bewährte Piercing-Technologie erübrigt sich aufwändiges Abisolieren und Konfektionieren von Buskabeln
- Nur ein AS-Interface Kabel zur sicheren und nichtsicheren Kommunikation
- Somit nur eine Schnittstelle zu HMI-Systemen
- Es wird keine zusätzliche TÜV-Abnahme der Programmbausteine benötigt.
- Sehr einfache Programmierung durch graphisches hardwareorientiertes Tool (vgl. Abschnitt 4).
- Einfache Einbindung von Hardware wie Not-Halt-Schalter, Schutztür-Schalter oder Sicherheits-Lichtgitter direkt durch integrierte AS-Interface Slaves

Highlights

- Geringerer Aufwand für Engineering
- Sehr einfache und schnelle Inbetriebnahme
- Reduzierte Kosten, da keine fehlersichere Steuerung benötigt wird
- Effizientere Betriebsphase durch integrierte Diagnose
- Reaktionszeit 40 ms

Mit ASIsafe profitieren:
- Maschinen- und Anlagenbauer durch Kosteneinsparungen und
- Anlagenbetreiber durch höhere Anlagenverfügbarkeit und hohe Flexibilität

Anwendungsbereich

ASIsafe wird erfolgreich in verschiedenen Applikationen über sämtliche Branchen hinweg eingesetzt.

Folgende Aufgabenstellungen wurden beispielsweise mit ASIsafe erfolgreich abgesichert:

- Gütertransport über Förderbänder
- Pressen
- Bearbeitungszentren in der Automobilindustrie
- Werkzeugmaschinen
- Personentransport über Rolltreppen
- Papiermaschinen
- Verpackungsmaschinen in der Nahrungs- und Genussmittelindustrie

Prinzipieller Aufbau und Funktion

Das folgende Bild zeigt den Grundaufbau von ASIsafe

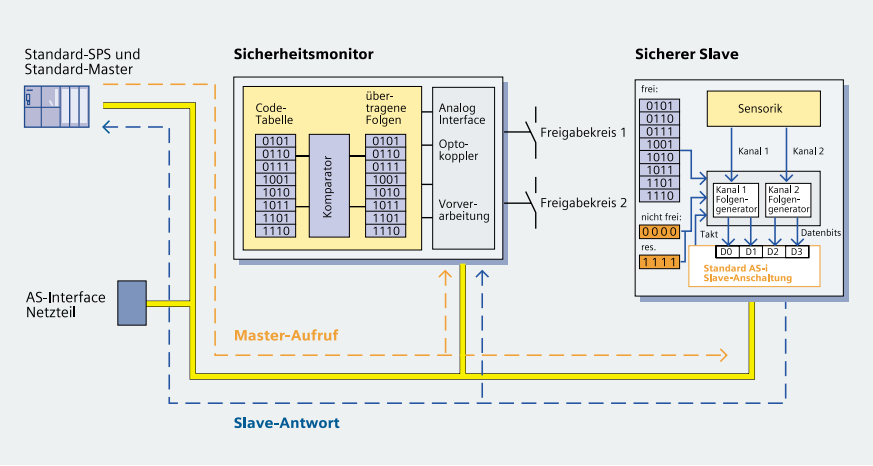


Bild 4/9
Grundaufbau von ASIsafe

Ein herkömmliches AS-i Netz besteht aus Steuerung/Master, Netzteil, dem gelben AS-i-Kabel sowie verschiedenen Slaves. Nur zwei weitere Komponenten sind für sichere Anwendungen nötig: Ein Sicherheitsmonitor und sichere Slaves.

Basis der sicheren Datenübertragung ist ein dynamisiertes sicheres Übertragungsprotokoll.

In jedem sicheren Slave ist werkseitig eine Codetabelle hinterlegt, die diesen für den Sicherheitsmonitor eindeutig identifizierbar macht. Jeder sichere Slave muss im Sicherheitsmonitor parametriert werden, indem der Anwender die Aufforderung „sicheren Slave teachen“ bestätigt. Seine zugehörige Codetabelle wird dann im Vergleicher des Sicherheitsmonitors abgespeichert. Mit jedem Masteraufruf wird die Übereinstimmung der vom Vergleicher erwarteten Code-Werte mit den tatsächlich erwarteten Code-Werten überprüft. Bei Abweichungen oder Zeitüberschreitungen erfolgt am Sicherheitsmonitor die sichere Abschaltung über 2-kanalig ausgeführte Freigabekreise.

Für gezieltes Abschalten ist der Code-Wert „0000“ reserviert. So wird z.B. bei Betätigen eines Not-Halt-Tasters die „0000“ an den Sicherheitsmonitor gesendet, worauf dieser ebenfalls eine sichere Abschaltung über den entsprechenden Freigabekreis vornimmt.

Mit der für AS-Interface typischen Masterabfrage erhält der Sicherheitsmonitor die sicherheitsrelevanten Codetabellen. Master und SPS bekommen diese Information lediglich mitgeteilt, ohne dabei eine aktive Rolle zu spielen. So ist z.B. eine zusätzliche Auswertung der Informationen zu Diagnosezwecken über die Anlagensteuerung möglich.

Funktionen des Sicherheitsmonitors

Der AS-Interface Sicherheitsmonitor wertet die sicheren Eingänge der Sicherheitsslaves und die Eingänge aus dem Rückführkreis aus (siehe Bild 4/10). Er verknüpft diese über Logikbausteine. Hieraus wird die sichere Ausgabe der Freigabekreise eines Sicherheitsmonitors ermittelt.

Der Sicherheitsmonitor läuft dabei abhängig von den parametrierten Startbausteinen unterschiedlich an.

Der AS-Interface Sicherheitsmonitor besitzt eine breite Vielfalt an Funktionsbausteinen, welche unterschiedlichste Anlagenkonfigurationen ermöglichen.

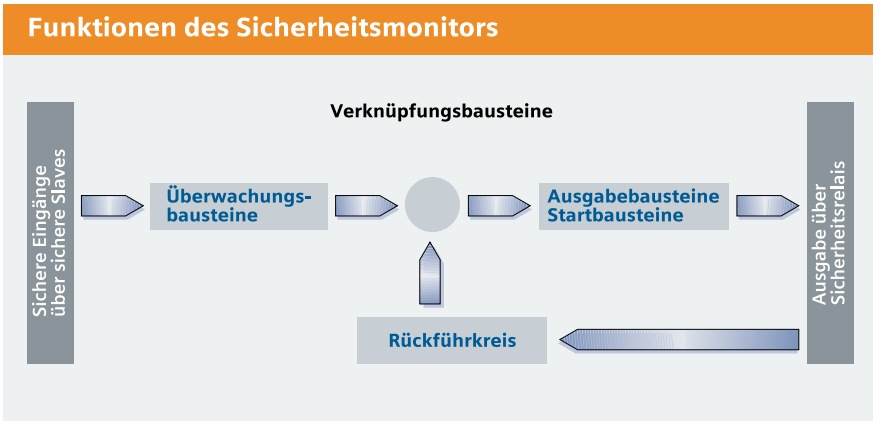


Bild 4/10
Funktionen des Sicherheitsmonitors

Überwachungsbausteine:

Die sicheren Slaves können über folgende Überwachungsbausteine parametriert werden:

Alle Überwachungsbausteine können zusätzlich auf Anlauftests und Vor-Ort-Quittierung parametriert werden.

Überwachungsbausteine	Funktion	Beispiele
Zweikanalig zwangsgeführt	Zwei redundante Kontakte; müssen gleichzeitig betätigt werden	Not-Halt nach Kategorie 3/4 (EN 954-1)
Zweikanalig abhängig	Zwei redundante Kontakte; Beide müssen nach einer Sychronisationszeit geöffnet/geschlossen sein	Zweihandbedienungen; Schutztüren mit zwei Sicherheitsschaltern
Zweikanalig abhängig mit Entprellung	Zwei redundante Kontakte; Beide müssen nach einer Prell- und Synchronisationszeit geöffnet/geschlossen sein	Schleichschalter Schalter mit hohen Prellzeiten
Zweikanalig bedingt abhängig	Zwei redundante Kontakte; Ein Kontakt dient zur Überwachung, der zweite Kontakt dient zur Verriegelung und Überwachung	Türschalter mit Verriegelung
Zweikanalig unabhängig	Zwei unabhängige Schaltsignale wirken auf die Eingänge eines Sicherheitsslaves	Schutztürüberwachung nach Kategorie 2 (EN 954-1)
Standard Slave	Betriebsmäßiges Schalten	-
Taste	Vor-Ort-Quittierung mehrerer Bausteine	Gemeinsame Quittierung von Lichtgittern
NOP (No Operation)	Platzhalter für einen Baustein zum Erhalt der Bausteinindizes	Gleiche erweiterte Diagnose kann für unterschiedliche Anlagenkonfigurationen beibehalten werden

Tabelle
Sicherheitsklassen bei den verschiedenen Aufbauvarianten

Verknüpfungsbausteine:

Zur logischen Verknüpfung der sicheren Eingänge können die folgenden Funktionen gewählt werden:

- UND
- ODER
- Flip-Flop
- Einschalt- und Abschaltverzögerungen bis zu 300 s
- Impulse

Rückführkreis-Bausteine:

Diese Bausteine ermöglichen die Überwachung des Zustands der nachgeschalteten Motorschütze zur dynamischen (online) Kontrolle.

Mittels dieser Bausteine kann auch ein Fernreset des Sicherheitsmonitors bei Fehlern eingestellt werden

Ausgabebausteine:

Diese Bausteine beschreiben, wie ein sicherer Halt ausgeführt werden soll.
Es können:
- Stopkategorie 0 (sofortiger Stop)
- Stopkategorie 1 (verzögerter Stop bis zu 300 s)
- Türzuhaltungen mit und ohne Stillstandswächter (bei zwei bedingten Freigabekreisen eines Monitors)

eingestellt werden.

Start-Bausteine:

Diese Bausteine ermöglichen einen definierten Anlauf einer Anlage.
Es sind die folgenden Einstellungen möglich:

Automatischer Wiederanlauf
- Überwachter Start mittels Quittierung durch Standard AS-i Slave
- Überwachter Start mittels Eingang Start am Sicherheitsmonitor
- Überwachter Start mittels Quittierung durch sicheren AS-i Slave

Die Parametrierung der Sicherheitstechnik ist dabei intuitiv einfach gelöst: Die Bausteine werden einfach per drag & drop in den entsprechenden Freigabekreis des Sicherheitsmonitors gezogen.

Durch Doppelklick des entsprechenden Bausteins kann dieser über ein Dialogfenster weiter konfiguriert werden.

Einfache Konfiguration von ASIsafe mit asimon

Jeder Monitor kann mittels der Konfigurationssoftware asimon einfach mit dem PC konfiguriert werden. Der PC wird über ein entsprechendes Kabel mit dem Sicherheitsmonitor verbunden.

Die Sicherheitslogik wird per drag & drop parametriert.

Dazu wird für jede Sicherheitsfunktion die entsprechenden grafischen Sicherheitskomponenten einfach aus dem Katalog in den auszulösenden Freigabekreis des Sicherheitsmonitors gezogen (siehe Bild 4/11).
Hierbei können die Betriebsmodi sowie weitere Funktionen wie Türzuhaltungen, Stop-Kategorie 0 und 1, Schützkontrolle, Wiederanlaufsperre, Vor-Ort-Quittierung und Zustimmschalter eingestellt werden.

Zudem sind Logikbausteine wie UND und ODER vorhanden.

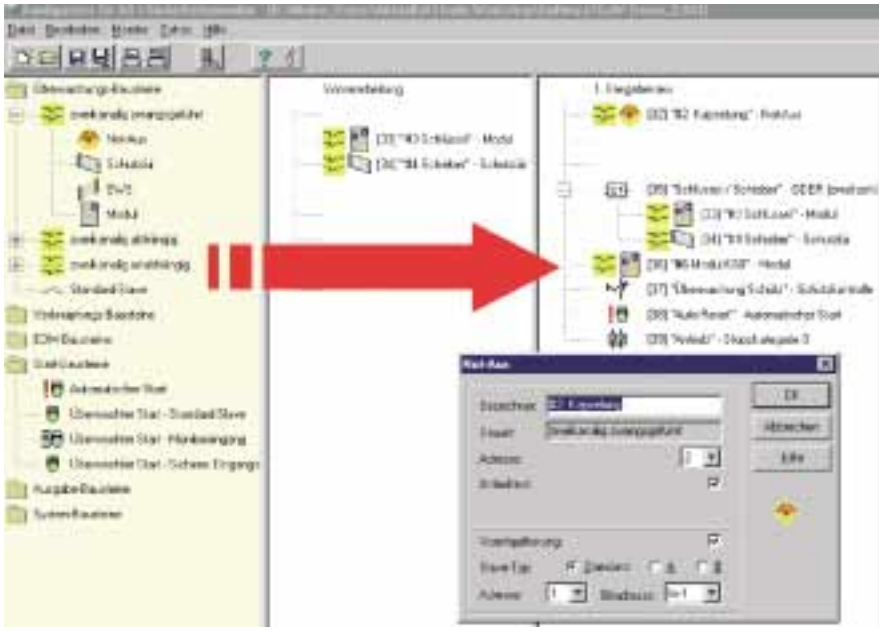


Bild 4/11
Konfigurationssoftware asimon

Einbindung sicherer Signale zwischen zwei AS-Interface Netzen

Zwischen zwei ASIsafe Netzen ist der Austausch sicherer Daten möglich.

Hierzu wird ein Freigabekreis eines Sicherheitsmonitors aus Netz 1 auf einen sicheren Eingang an einem Modul aus Netz 2 verdrahtet.

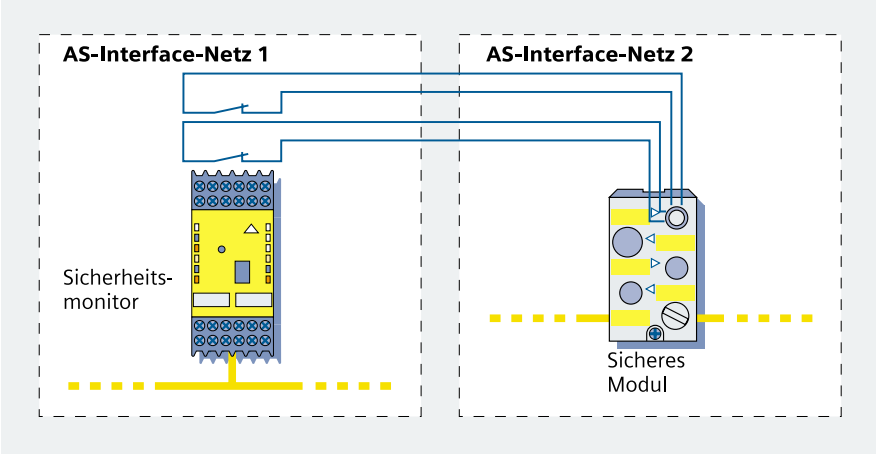


Bild 4/12
Austausch sicherer Daten zwischen zwei ASIsafe Netzen

Gruppierung sicherer Signale mit ASIsafe

ASIsafe ermöglicht die Gruppenbildung sicherer Signale.

Die Darstellung zeigt ein Netz, das neben den bekannten Standard-Komponenten zwei Sicherheitsmonitore mit je einem 2-kanaligen Freigabekreis und vier sicheren Slaves enthält. Jeder Monitor ist beispielsweise einem Anlagenteil zugeordnet, der über den entsprechenden Freigabekreis abgeschaltet werden kann.

Die Zuordnung der sicheren Slaves zu den Sicherheitsmonitoren wird über PC konfiguriert.

Das Beispiel ist so konfiguriert, dass das sichere Modul und Not-Halt 1 auf Sicherheitsmonitor 1 wirken. Wird z.B. Not-Halt 1 gedrückt, so wird der dem Monitor zugeordnete Anlagenteil über den entsprechenden Freigabekreis abgeschaltet.

Not-Halt 2 wirkt auf beide Sicherheitsmonitore, d.h., eine Betätigung von Not-Halt 2 schaltet beide Anlagenteile ab.

Not-Halt 3 wirkt nur auf Sicherheitsmonitor 2 und schaltet den hier zugeordneten Anlagenteil ab.

Wie in dem Beispiel gezeigt, können in einem AS-Interface-Netz auch mehrere Sicherheitsmonitore verwendet werden. So ist nicht nur Gruppenbildung möglich, auch die Kombination verschiedener Betriebsmodi in einem Netz ist so durchführbar.

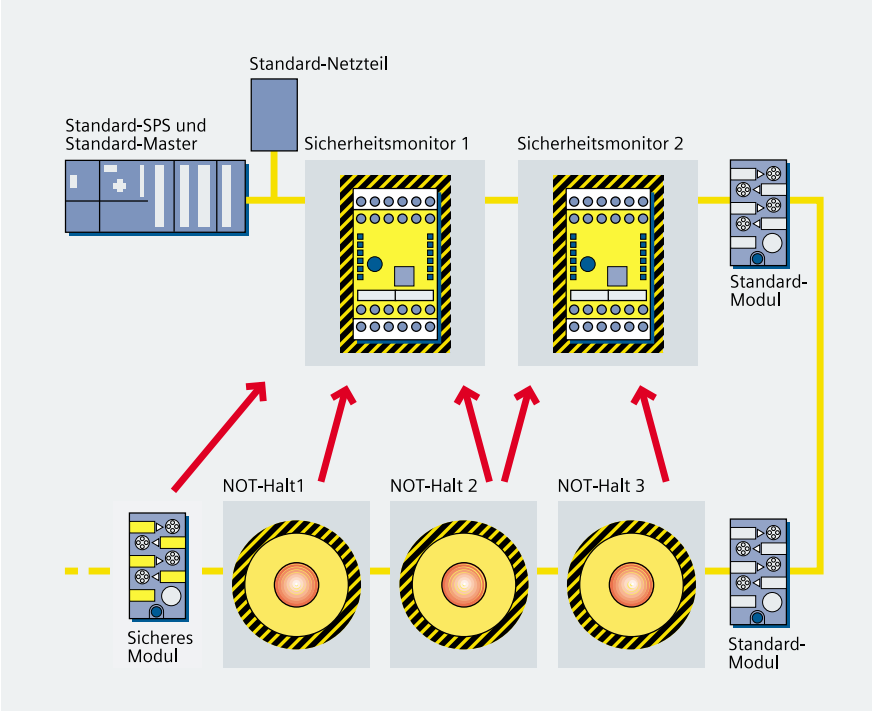


Bild 4/13
Gruppenbildung sicherer Komponenten

Integration in TIA

AS-Interface Netze mit ASIsafe

Ein ASIsafe–Netz mit Safety at Work-Komponenten kann einer dezentralen Peripherie-Station ET 200S unterlagert werden. Hierzu wird ein Freigabekreis eines Sicherheitsmonitors in den Sicherheitskreis der ET 200S durch Verdrahtung eingeschleift. Zur Reaktionszeit von ASIsafe (max. 40 ms) addiert sich die Reaktionszeit der ET 200S SIGUARD um 20 ms.

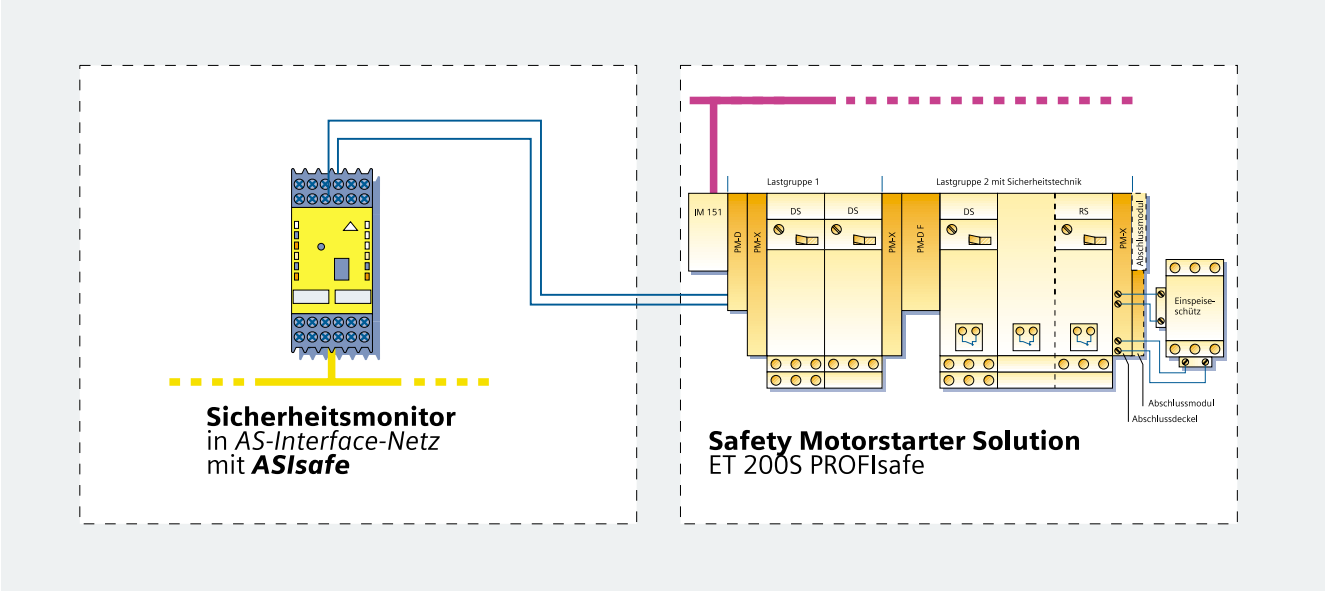


Bild 4/14
ASIsafe unter ET 200S Motorstarter

Einfache Diagnose

Wird ein sicherer Slave ausgelöst, so übermittelt dieser die Daten „0000“.

Diese Information liegt am Master vor und kann einfach durch die Steuerung ausgewertet werden.

Detaillierte Diagnose

Über die reine asimon-Konfigurations-Software hinaus, liefert Siemens auf der ASIsafe CD-ROM auch Funktionsbausteine für die S7-200 und S7-300 aus. Mit diesen ist eine detaillierte Diagnose aller parametrierten Bausteine möglich (siehe Bild 4/15).

Dazu muss an den Sicherheitsmonitor eine AS-i Adresse über die Konfigurationssoftware vergeben werden. Die Auswertung erfolgt über Funktionsbausteine in der SPS.

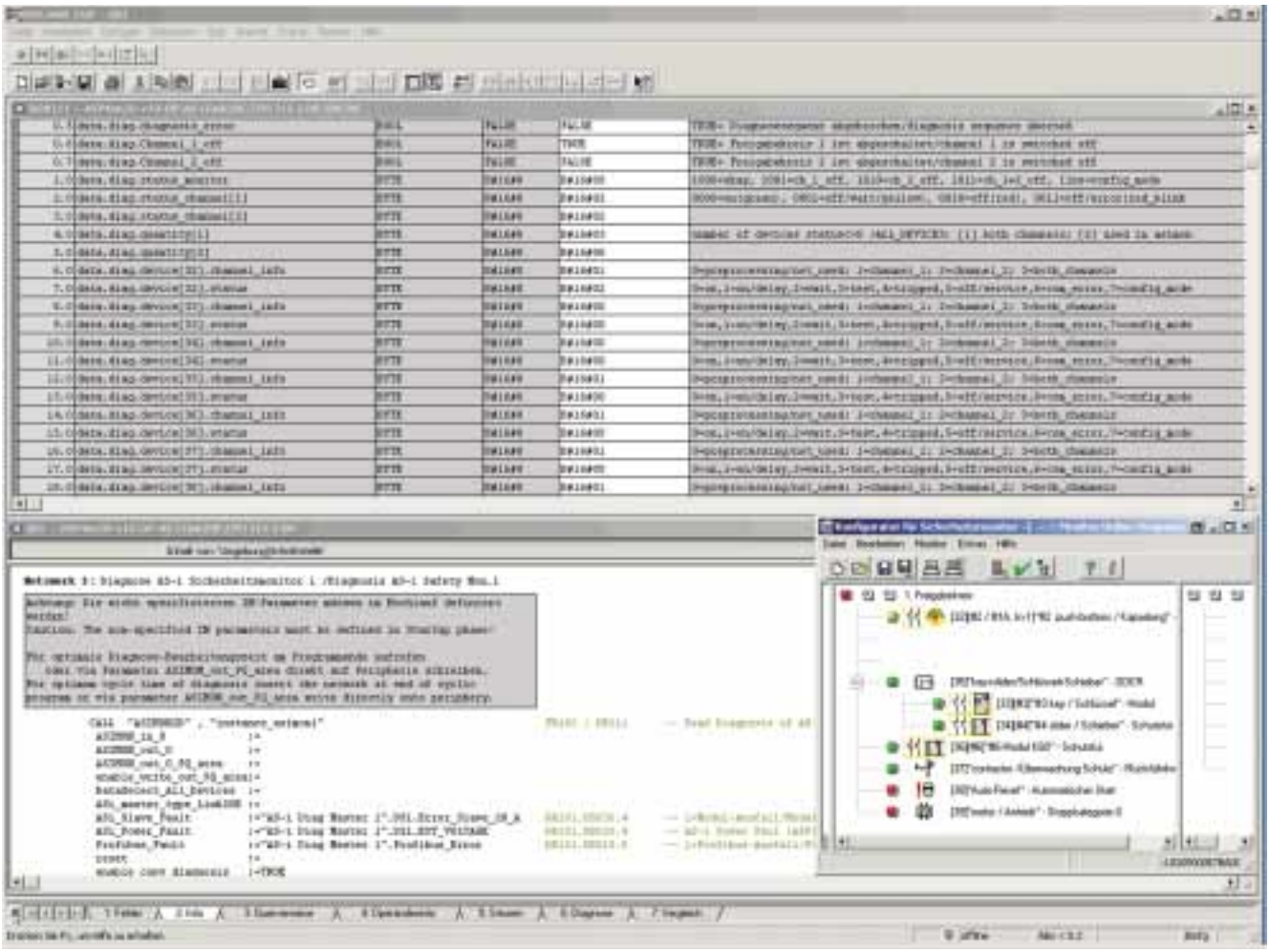
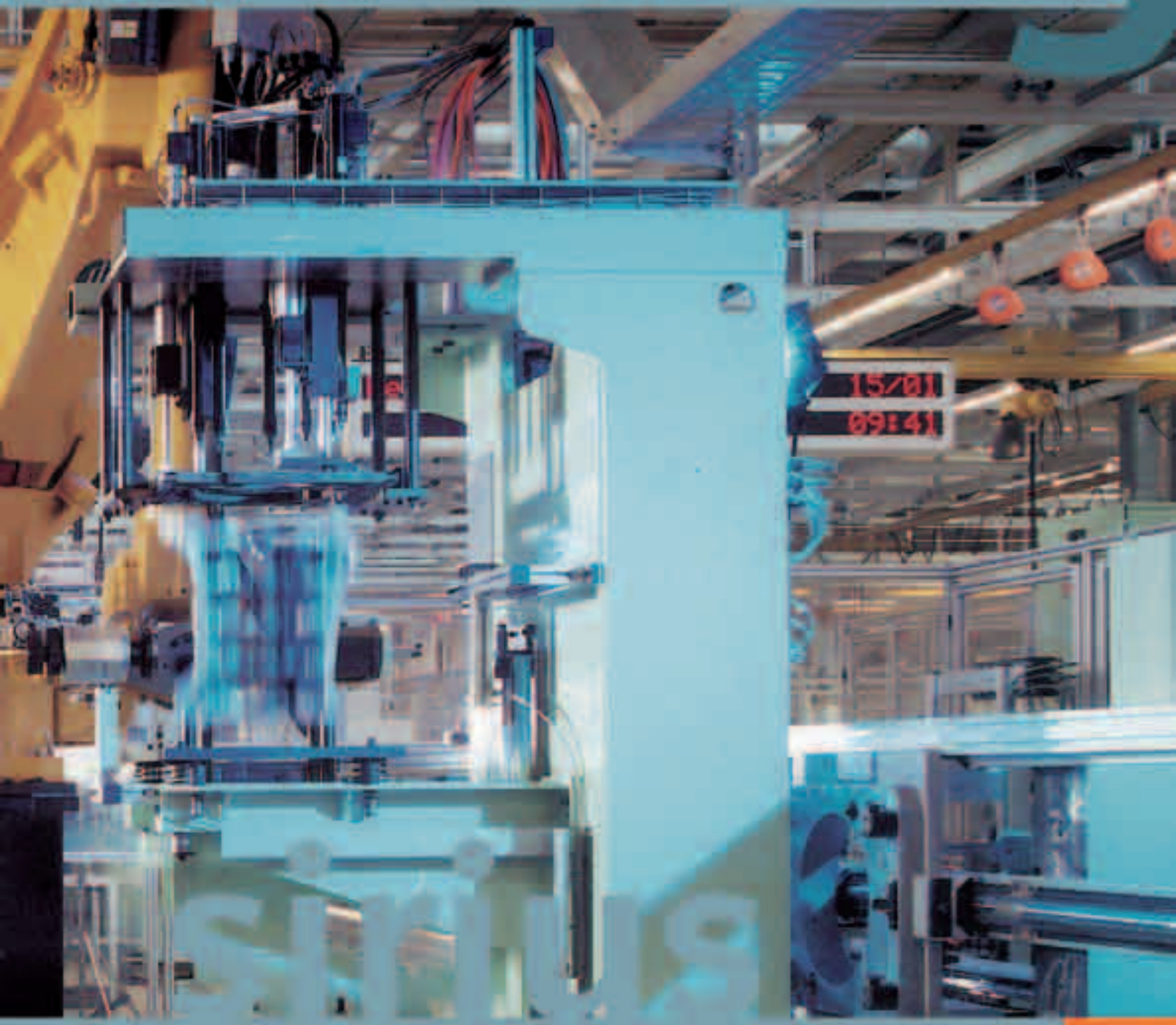


Bild 4/15
Funktionsbaustein zur Detail-Diagnose des ASIsafe Netzes in der SPS

5.1 SIRIUS Positionsschalter
5.2 SIRIUS Not-Halt
5.3 SIRIUS Befehls- und Meldegeräte
5.4 SIRIUS Sicherheitsschalttechnik
5.5 ASIsafe
5.6 ET 200S Safety Motorstarter Solution

Sicherheitsgerichtete Schalttechnik



5 Sicherheitsgerichtete Schalttechnik

5.1 SIRIUS Positonsschalter

Übersicht

SIRIUS Positionsschalter dienen zur

- Positionserfassung von beweglichen Maschinenteilen
- Erfassung von gefährlichen Bewegungen von Maschinenteilen
- Überwachung von Schutzeinrichtungen mit Drehgelenken wie Schwenktüren, Klappen, Deckel usw.
- Überwachung von seitlich verschiebbaren Schutzeinrichtungen wie Schiebetüren, Schutzgitter usw.

Merkmale

SIRIUS Positionsschalter bieten

- Ein umfangreiches Produktspektrum mit standardisierten Gehäusen und Antriebsformen
- Einfach montierbare Lösungen für die Erfassung sowie Überwachung von gefährlichen Bewegungen und Zugangsbereichen.
- Standardisierte Gerätebefestigung nach Norm EN 50041 bzw. EN 50047
- Maximalen Schutz gegen Umgehung bzw. Manipulation der Schutzeinrichtung durch z.B. mehrfach kodierte, getrennte Betätiger
- Überwachung von Schutzeinrichtungen bis Kategorie 4 nach EN 954-1
- Integration in das Bus-System ASIsafe
- Hohe Schutzart bereits bei Standardprodukten

Anwendungsbereich

SIRIUS Positionsschalter werden u.a. für folgende Aufgabenstellungen eingesetzt:

- Im Anlagen- und Maschinenbereich bei der Überwachung von Schutzumzäunungen und Zugangsklappen an Druckmaschinen.
- Positionsschalter mit Zuhaltung werden in erster Linie zur Überwachung von Maschinenbereichen mit erhöhtem Gefährdungspotenzial wie Roboterzellen eingesetzt. Sicheres Zuhalten einer Schutztür bis zum Maschinenstillstand.
- Sicheres Abschalten einer Anlage beim Erreichen der Endlage, z.B. bei Aufzügen oder Fahrtreppen.
- Manipulationssichere Schutztürüberwachung mittels Magnetschalter bei verdecktem Einbau des Schalters, auch in Bereichen in denen Reinigung und Desinfektion eine große Rolle spielt.

Standard-Positionsschalter

Durch eine Vielzahl praxisorientierter Antriebe, Gehäuse und Kontaktsystemen überzeugen die Positionsschalter SIRIUS 3SE in nahezu allen Applikation.
Mit zwangsöffnenden Öffnerkontakten.
Ausführungen mit Abmessungen, Befestigungspunkte und Kennwerte entsprechend der Normen EN 50041 bis EN 50047 sind verfügbar.

Die Kurzhubschalter sorgen mit ihrem deutlich reduziertem Schaltweg und präzisen Schaltpunkten für ein sicheres Abschalten auch bei sehr kurzen Betätigungswegen.

Positionsschalter mit getrenntem Betätiger/Zuhaltung

Für die Überwachung von Schutztüren stehen eine große Anzahl von Gehäuse- und Betätigervarianten zur Verfügung. Durch die mehrfach mechanisch kodierten Betätiger ist ein Umgehen der Schutzeinrichtung mit einfachen Mitteln auszuschließen.
Mit zwangsöffnenden Öffnerkontakten.
Zuhaltung:
Positionsschalter mit getrenntem Betätiger und Zuhaltung halten eine Schutztür verriegelt, bis der Arbeitsbereich ohne Gefahr betreten werden kann. Ein elektrisches Signal, z.B. von einem Stillstandswächter, steuert den Verriegelungsmagneten an und gibt somit die Schutztür frei.

Federkraftverriegelte (Ruhestromprinzip) sowie magnetkraftverriegelte (Arbeitsstromprinzip) Ausführungen mit standardmäßig 4 Kontakten stehen zur Verfügung.

Schanierschalter

Ausführungen im Normgehäuse nach EN 50047 für die mechanische Anbindung an die Scharnierachse, sowie Scharnierschalter mit bereits montiertem Scharnier sind verfügbar.
Mit zwangsöffnenden Öffnerkontakten.
Bereits bei Öffnungswinkeln der Schutztür von 4 Grad öffnen die Öffnerkontakte und geben den Befehl zum Abschalten. Bei den Ausführungen mit Sprungkontakten wird zeitgleich zum Abschaltbefehl (Öffnerkontakt) auch der Meldebefehl (Schließerkontakt) gegeben.

Magnetschalter

Die berührungslos arbeitenden Magnetschalter bieten einen hohen Schutz gegen Manipulation. Sie stehen in 3 verschiedenen Bauformen zur Verfügung.

Die sichere Auswertung bzw. Überwachung zum Erreichen der Kategorie 4 nach EN 954-1 erfolgt über die Sicherheitsgeräte 3TK284, 3SE6, ASIsafe und F-SIMATIC.

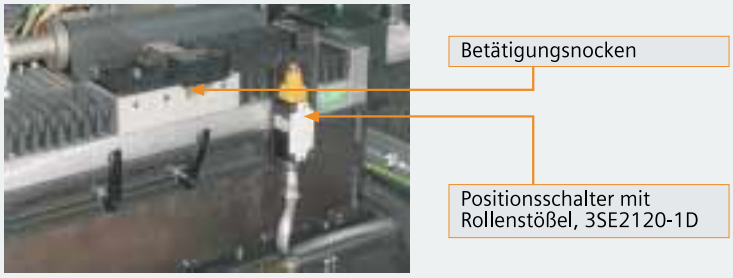
Aufbau

- Standardschalter:
  modularer Aufbau mit austauschbaren Baugruppen (Antriebskopf, Gehäuse, Schalelemente).
- Getrennte Betätiger sowie Schalter mit Zuhaltung:
  feste Schaltereinheit mit unterschiedlichen Betätigern kombinierbar (Standardbetätiger, mit seitlicher Befestung und Radiusbetätiger).
- Scharnierschalter:
  kompakte Schaltereinheit zur Direktmontage an die Scharnierachse bzw. mit bereits vormontiertem Scharnier.
- Standardanschluss für mechanische Positionsschalter:
  metrische Anschlussverschraubung, vorzugsweise M20x1,5. Varianten mit M12 Stecker und mehrpoligen Steckern verfügbar.
- Magnetschalter:
  kompakte, vergossene Geräteeinheit mit bereits angeschlossener Anschlussleitung.

Beispiele

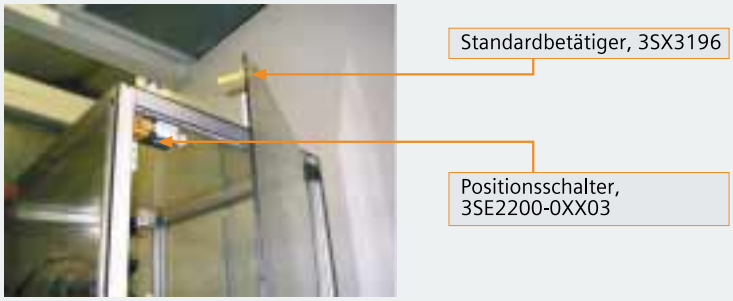
1. Standardschalter:

Endlagenerfassung an Werkzeugschlitten im Sondermaschinenbau



2. Schalter mit getrenntem Betätiger:

Schutztürüberwachung bei automatischen Fertigungseinrichtungen



3. Scharnierschalter:

Überwachung von Zugangsklappen bei Holzbearbeitungsmaschinen

4. Magnetschalter:

Mögliche Kombination Überwachungseinheit – Magnetschaltersytem

Mögliche Kombination Überwachungseinheit – Magnetschalter

Überwachungseinheit	**Magnetschalter** 1Ö/1S			**Magnetschalter** 2Ö
	Schaltelement 3SE6 605-1BA (M30)	**Schaltelement 3SE6 605-2BA** (25 x 33 mm)	**Schaltelement 3SE6 605-3BA** (25 x 88 mm)	**Schaltelement 3SE6 604-2BA** (25 x 88 mm)
	Schaltrelais 3SE6 704-1BA	**Schaltrelais 3SE6 704-2BA**	**Schaltrelais 3SE6 704-3BA**	**Schaltrelais 3SE6 704-2BA**
Relaisausgang SIRIUS-Sicherheitsschaltgerät, 6-fach [1] 3SE6 806-2CD00	•	•	•	–
Elektronikausgang SIRIUS-Sicherheitsschaltgerät, Elektronik [2] 3TK284.	–	–	–	•
SIRIUS-Sicherheitsschaltgerät, mit Hilfsschütz, Elektronik [2] 3TK285.	–	–	–	•
SIRIUS-Sichere Verbraucherabzweige Elektronik [2] 3RA7.	–	–	–	•
ASIsafe [2] 3RK1.	–	–	–	•
SIMATIC ET 200S [2] PROFIsafe [2] 4/8F-DI DC24V	•	•	•	•
SIMATIC ET 200M [2] SM326, DI DC24V SIMATIC S7 300F [2] SM326, DI 8 x Namur	•	•	•	•

[1] Kat.3 erreichbar nach EN 954

[2] Kat.4 erreichbar nach EN 954

Technische Daten

SIRIUS Positionsschalter	
Standard-Positionsschalter	• **Zwangsöffnung der Öffnerkontakte, gemäß IEC 947-5-1** • **Hohe Kontaktzuverlässigkeit auch bei 5V DC / 1mA** • **Geeignet für Umgebungstemperaturen von -35° bis +85°C** • **Sehr hohe mechanische Lebensdauer (30 Mio. Schaltungen)** • **hohe Schutzart IP67** • Verschiedene Ö/S Kontaktvarianten, bis zu 4 Kontakte möglich • Gehäuse nach EN 50041, EN 50047 und Sonderbauformen
Positionsschalter mit getrenntem Betätiger/ Zuhaltung	• **Formstoff-, bzw. Metallgehäuse in IP66 und IP67** • **Gehäuse nach EN 50047, EN 50041 und Sonderbauformen** • **Sicherheitsstandard für Schutztürverriegelungen nach EN 1088** • **Anfahrmöglichkeiten aus 4 bzw. 5 Richtungen** • **Hohe Schutzart IP65 bzw. IP67** • **Mechanische Lebensdauer $1x10^6$ Schaltungen** • **Umgebungstemperatur von -30^o bis $+85^oC$** • Verschiedene Ö/S Kontaktvarianten, bis zu 4 Kontakte möglich, sowie Stellungsüberwachung des Betätigers und des Verriegelungsmagneten mit bis 2 Kontakten.
Scharnierschalter	• Gehäuse nach EN 50047 für Scharniermontage 1S/1Ö Sprung, 5 Grad der 15 Grad Schaltpunkt • Schalter mit integriertem Scharnier für 40 mm Profile, Schaltpunkt 4 Grad, 5 oder 15 Grad, 1S/2Ö Schleichschaltglieder

5.2 SIRIUS Not-Halt

Übersicht

Der SIRIUS Not-Halt Schalter dient dem manuellen Abschalten von Anlagen im Gefahrenfall und wird durch das Bedienpersonal veranlasst (nach ISO 13850 (EN 418)).

Merkmale

SIRIUS Not-Halt Schalter zeichnen sich aus durch:

- Umfangreiches Produktspektrum mit verschiedenen Not-Halt Bedienteilen
  - Drehentriegelung
  - Zugentriegelung
  - Entriegelung durch Schlüssel
- Einfach und schnell zu montieren
- Kunststoff- und Metallvarianten
- Eingebettet u.a. in das Bus-System AS-Interface

Es ergeben sich folgende Vorteile:

- Einsetzbar bis Kategorie 4 nach EN 954-1 aufgrund der zwangsöffnenden Öffnerkontakte
- Hohe Schutzart bis zu IP67
- Abgestimmtes Spektrum an Befehls- und Meldegeräten
- Direktanbindung an ASIsafe, Direktanschluss an die gelbe Profilleitung

Anwendungsbereich

Not-Halt Befehlsgeräte schaffen in Anlagen und Maschinen aller Art die Möglichkeit, im Gefahrenfall manuell abzuschalten und werden in folgenden Branchen eingesetzt:

- Allgemeiner Maschinenbau
- Automatisierungstechnik
- Sondermaschinenbau
- Holzverarbeitende Industrie
- Werkzeugmaschinenbau
- NUK

Produktfamilie/Produktgruppen

Die Produktfamilie der SIRIUS Befehlsgeräte umfasst neben Not-Halt Betätigern:

- Drucktaster
- Leuchtmelder
- Knebelschalter
- Schlüsselschalter
- Not-Halt-Befehlsgeräte

Die Geräte sind in runder oder quadratischer Kunststoffausführung sowie als runde Metallausführung erhältlich.

Die Not-Halt-Befehlsgeräte sind einsetzbar bis Kategorie 4 der EN 954-1. Sie verfügen alle über zwangsöffnende Öffnerkontakte.

Zur sicheren Auswertung bzw. Überwachung zur Erreichung der Kategorie 4 über Sicherheitsbaustein werden 3TK28, ASIsafe und F-SIMATIC eingesetzt.

Technische Daten

SIRIUS Not-Halt	
Schutzart	IP66 (Kunststoffausführungen) IP67 (Metallausführungen)
Befestigungsbohrung	22,3 mm+0,4 mm (Runde Ausführungen,Kunststoff und Metall) 26 x 26 mm (Quadratische Kunststoffausführungen)
Bemessungsbetriebsspannung	400 V, AC 12
Bemessungsbetriebsstrom	10 V, AC 12
Kontaktsicherheit (Prüfspannung, -strom)	5 V, 1 mA

Aufbau

Die Befehlsgeräte sind modular aufgebaut und bestehen aus Betätigungselemeten wie Not-Halt, Drucktaster sowie einem Halter zum Befestigen in der Fronttafelbohrung und den aufschnappbaren Schaltelementen und Lampenfassungen.

Das Betätigungselement wird in eine standardisierte 22,5 mm Frontplattenbohrung montiert und von hinten mit dem Halter befestigt. Schaltelemente und Lampenfassungen werden auf die Rückseite des Betätigungselementes aufgeschnappt.

Schaltelemente und Lampenfassungen sind verfügbar mit Schraubanschluss, Federzugklemme sowie mit Lötstiften zum Einlöten in Leiterplatten.

Beispiel

Automatisierte Fertigungslinie mit an exponierten Stellen platzierten Not-Halt Befehlsgeräten zum manuellen Abschalten der Linie oder Module der Linie im Gefahrenfall.

5.3 SIRIUS Befehls- und Meldegeräte

Übersicht

SIRIUS Befehlsgeräte dienen dem manuellen Abschalten von Anlagen im Gefahrenfall und wird durch das Bedienpersonal veranlasst. Hierfür stehen die klassischen Not-Halt Befehlsgeräte (nach ISO 13850 (EN 418)) zur Verfügung.

SIRIUS Meldegeräte dienen zur visuellen und akustischen Meldung des Maschinen- oder Anlagenzustands. Meldegeräte sind für das modulare Programm „SIRIUS Befehls-und Meldegeräte 3SB3“ sowie auch als Signalsäulen 8WD mit umfangreichen Zubehör erhältlich.

Merkmale

SIRIUS Befehlsgeräte bieten:

Not-Halt Drucktaster 3SB3

- Umfangreiches Produktspektrum mit verschiedenen Not-Halt Bedienteilen - Dreh-, Zug- und Schlüsselentriegelung
- Not-Halt Funktion nach ISO 13850 (EN 418)
- Einfach und schnell zu montieren
- Kunststoff- und Metallvarianten
- Ein-Mann Montage ohne Sonderwerkzeug
- Modulare Bestückung der Betätigungselemente
- Umfangreiches Zubehör
- Eingebettet u.a. in das Bussystem AS-Interface

Zweihandbedienpulte 3SB3

- Normgerechte Lösung nach EN 574 und DIN 24980
- Not-Halt Funktion nach ISO 13850 (EN 418)
- Kunststoff- und Metallvarianten
- Robuste Metallausführung für härteste Einsatzbedingungen
- Nachrüstbare AS-Interface Lösung

Seilzugschalter 3SE7

- Not-Halt Funktion nach ISO 13850 (EN 418)
- Ausführungen für Seillängen bis zu 100 m
- LED Signalanzeige mit hoher Leuchtkraft
- Überwachung von Seilriss und Seilzug
- Integrierter ASIsafe

Fußschalter 3SE29

- Rastfunktion nach ISO 13850 (EN 418)
- Robuste Metallvarianten sowie kostengünstige Kunststoff-Pedaltaster
- Mit und ohne Schutzhaube lieferbar

SIRIUS Befehlsgeräte bieten:

Not-Halt Drucktaster 3SB3

- Einbettung in das montagefreundliche Programm „SIRIUS Befehls- und Meldegeräte 3SB3“
- Verschiedene Farben in Glühlampen und LED Technik
- Kunststoff- und Metallvarianten
- Hohe Schutzart IP67 und NEMA4

Signalsäule 8WD4

- Modularer Aufbau, bis zu 5 Module pro Säule
- Einfache Montage, Lampenwechsel ohne Werkzeug
- Anbindung an AS-Interface
- Hohe Schutzart IP65
- Umfangreiches Zubehör

Anwendungsbereich

SIRIUS Befehls- und Meldegeräte schaffen in Anlagen und Maschinen aller Art die Möglichkeit, im Gefahrenfall manuell abzuschalten und werden überwiegend in nachfolgenden Branchen eingesetzt.

- Allgemeiner Maschinenbau
- Automatisierungstechnik
- Sondermaschinenbau
- Holzverarbeitende Industrie
- Werkzeugmaschinenbau
- NUK

Seilzugschalter werden an ausgedehnten Anlagen wie z.B. Transportbändern im Tagebergbau oder Materialzuführungsbändern bei Druckmaschinen eingesetzt.

Produktfamilie/Produktgruppen

Befehls- und Meldegeräte 3SB3

Das komplette 3SB3 Programm umfasst ein sehr umfangreiches Spektrum für die Fronttafelmontage sowie eine Vielzahl von standardisierten als auch kundenspezifischen Kapselungen.

Für das gesamte Programm existieren Lösungen zur Anbindung an AS-Interface.

Zweihandbedienpult 3SB3

Zur Ortsbindung beider Hände an Pressen und Stanzmaschinen stehen diverse Varianten in Kunststoff und Metall zur Verfügung. Montierbar direkt an der Maschine sowie auf einem Ständer (Zubehör). Standardmäßig sind die Zweihandbedienpulte mit zwei Bedientaster und einem Not-Halt Pilzdrucktaster bestückt.

Seilzugschalter 3SE7

System aus Seilzugschalter und Seil.

Seilzugschalter gibt es je nach benötigter Seillänge in verschiedenen Bauformen. Bis zu 100 m Seillänge sind möglich. Für jede Bauform sind unterschiedliche Kontaktbestückungen verfügbar.
Um den Zustand des Seilzugschalters weithin sichtbar zu machen kann der Schalter mit einer LED- Signalanzeige bestückt werden.
Umfangreiches Zubehör.

Fußschalter 3SE29

Fußbetätigte Befehlgeräte in 1- oder 2-pedaliger Ausführung mit tastenden und rastenden Kontaktelementen.
Zum zusätzlichen Schutz sind die Fußschalter auch mit einer robusten Schutzhaube verfügbar.

Signalsäulen 8WD

Verfügbare Elemente:
Dauerlicht, Blitz-, Rundumlicht, Blinklicht und Sirenenelemente
Verfügbare Farben: Rot, Gelb, Grün, Blau, Klar (Weiß)
Geräteanschluss in Schraub- und Cage Clamp Technik.
Bis zu 5 Elemente können pro Signalsäule montiert werden. Über das integrierbare ASI-Modul ist der Direktanschluss an das Bussystem AS-Interface möglich.
Diverse Akustikmodule bis zu 105 dB verfügbar.

Aufbau

Die SIRIUS Befehlsgeräte 3SB3 sind modular aufgebaut und bestehen aus Betätigungselemeten wie Not-Halt, Drucktaster sowie einem Halter zum Befestigen in der Fronttafelbohrung und den aufschnappbaren Schaltelementen und Lampenfassungen.

Das Betätigungselement wird in eine standardisierte 22,5 mm Frontplattenbohrung montiert und von hinten mit dem Halter befestigt. Schaltelemente und Lampenfassungen werden auf die Rückseite des Betätigungselementes aufgeschnappt.

Schaltelemente und Lampenfassungen sind verfügbar mit Schraubanschluss, Federzugklemme sowie mit Lötstiften zum Einlöten in Leiterplatten.

Technische Daten

SIRIUS Positionsschalter	
Befehl- und Meldegeräte 3SB3	• Schutzart IP66 (Kunststoffausführungen), IP67 (Metallausf.) • Befestigungsbohrung 22,3 mm+0,4 mm (Runde Ausführungen, Kunststoff und Metall), 26 x 26 mm (Quadratische Kunststoffausführungen) • Bemessungsbetriebsspannung 400 V, AC 12 • Bemessungsbetriebsstrom 10 V, AC 12 • Kontaktsicherheit (Prüfspannung, -strom) 5 V, 1 mA
Seilzugschalter 3SE7	• Metallgehäuse in Schutzart IP65 • Elektrische Belastung AC 15 AC 400 V, 6 A • Kurzschlussschutz 6A (träge) • Hohe Schutzart IP65 bzw. IP67 • Mechanische Lebensdauer >1x10^6 Schaltungen • Umgebungstemperatur von –25^o bis +70^{o}C • Verschiedene Ö/S Kontaktvarianten, bis zu 4 Kontakte möglich
Fußschalter 3SE29	• Metallgehäuse in Schutzart IP65 , Kunst • Elektrische Belastung AC15 AC 400 V, 6 A bzw. 16 A • Kurzschlussschutz 6 A (träge) bzw.16 A • Hohe Schutzart IP65 • Mechanische Lebensdauer >1x10^6 Schaltungen • Umgebungstemperatur von –25^o bis +80^{o}C • Verschiedene Ö/S Kontaktvarianten
Signalsäule 8WD	• Anschlusselement: schlagfestes Thermoplast Gehäuse • Lichtelemente: Thermoplast • Betriebsspannungen: 24 V AC/DC, 115 V AC und 230 V AC • Hohe Schutzart IP65 • Umgebungstemperatur von –30^o bis +50^{o}C

5.4 SIRIUS Sicherheitsschaltgeräte

Übersicht

Sicherheitsschaltgeräte werden eingesetzt, um auf eine Schaltanforderung (z.B. Betätigung von Not-Halt, Betreten eines gefährlichen Bereiches) die entsprechende Reaktion zum Schutz von Mensch, Maschine und Umwelt sicher und zuverlässig einzuleiten.

Typische Anlagen, in denen Sicherheitsschaltgeräte eingesetzt werden, kennzeichnen sich durch eine geringe Anzahl von Sensoren, eine geringere räumliche Ausdehnung sowie die Unabhängigkeit von einem Bussystem (Inselbetrieb) aus.

SIRIUS Sicherheitsschaltgeräte erfüllen einerseits die Anforderungen der einschlägigen Normen der Sicherheitstechnik, andererseits werden sie den Anforderungen der Industrie durch ihre kompakte Bauform und ihre Zuverlässigkeit gerecht. Sie sind ein wesentlicher Bestandteil des Siemens Sicherheitskonzeptes Safety Integrated.

Sie unterteilen sich in 2 Gruppen:
a) Sicherheitsschaltgeräte 3TK28
b) Sicherheitsgerichtete Verbraucherabzweige 3RA71

Merkmale

Die SIRIUS Sicherheitsschaltgeräte bieten dem Anwender eine Reihe von technischen Vorteilen. Sie sind aufeinander abgestimmt und kaskadierbar. Dieses erlaubt eine große Flexibilität bei der Erweiterung der Sicherheitsfunktionen in einer bestehenden Anlage. Alle Geräte, die zur Realisierung von Sicherheitsketten vom Sensor über die sichere Auswertung bis zum Aktor benötigt werden, finden sich im SIRIUS-Produktspektrum. Die kompakte Bauform der Sicherheitsschaltgeräte im SIRIUS-Design ermöglichen auch einen optisch angepassten Aufbau im Schaltschrank. Dass die SIRIUS Sicherheitsschaltgeräte weltweit zugelassen sind, ist besonders interessant für Exporteure von Maschinen. Ein großer Vorteil gerade für diese Kundengruppe ist auch, dass SIRIUS Sicherheitsschaltgeräte verschleißfrei arbeiten (elektronische Gerätefamilie) bzw. durch alternierende Schaltreihenfolgen (Geräte mit aufgesetzten Hilfsschützen und sichere Verbraucherabzweige) eine hohe Lebensdauer erreichen. Dadurch wird die Anzahl der Serviceeinsätze erheblich reduziert.

Die Merkmale auf einen Blick:

SIRIUS Sicherheitsschaltgeräte:

- überwachen die Sicherheitsfunktionen
- sind notwendiger Bestandteil der Sicherheitskette
- schützen Mensch, Maschine und Umwelt

Anwendungsbereich

SIRIUS Sicherheitsschaltgeräte werden dort eingesetzt, wo eine zuverlässige Auswertung von Sensorsignalen und das sicherheitsgerichtete Abschalten von gefährlichen Zuständen (Gefahren) erforderlich sind, z.B.

- Überwachung von Bereichen mit gefährlichen Bewegungen, z.B. Schutztür, Lichtgitter, Lichtschranke
- Überwachung des Fahrweges von Flurförderfahrzeugen mit Laserscanner
- Sicheres Stillsetzen bzw. Abschalten nach einer Not-Halt Anforderung

Diese Anwendungen findet man u.a.

- in der Automobilindustrie und deren Zulieferern
- im Allgemeinen Maschinenbau
- bei Papier-/Druckmaschinenherstellung
- in der Fördertechnik
- in der Nahrungsmittel- und Genussindustrie

Produktfamilie/Produktgruppen.

Die Familie der SIRIUS Sicherheitsschaltgeräte gliedert sich in Geräte mit einfacher und mittlerer Funktionalität. Geräte mit einfacher Funktionalität besitzen einen Eingang für den Anschluss eines Sicherheitssensors. Beim Auslösen des Sensors werden alle sicherheitsgerichteten Freigabekreise unverzögert oder zeitverzögert abgeschaltet. Geräte mit mittlerer Funktionalität haben zwei oder mehrere Sensoreingänge. Die sicherheitsgerichteten Freigabekreise dieser Geräte sind über eine Sicherheitslogik den Sensoreingängen zugeordnet.

Die Sicherheitsschaltgeräte der Familie 3TK28 / 3RA71 erfüllen je nach äußerer Beschaltung die Sicherheitsanforderungen bis Kategorie 4 nach EN954-1 bzw. SIL 3 nach IEC 61508 (Detailinformationen zu den einzelnen Geräten befinden sich im Katalog LV10 Bestell-Nr.: E86060-K1002-A101-A4).

SIRIUS Sicherheitsschaltgeräte können ohne Verwendung von Softwaretools parametriert werden. Durch voreingestellte Funktionalitäten sind die Geräte sofort nach der Montage betriebsbereit.

Sicherheitsschaltgeräte

- einfache Funktionalität
  - Relaiskontakt-Freigabekreise
    - Grundgeräte 3TK282.
    - Erweiterungsgeräte 3TK2830
    - Pressensteuergeräte 3TK2834-35
  - elektronische Freigabekreise
    - Basisgeräte 3TK2840
    - Grundgeräte 3TK2841-42
  - Hilfsschützkontakt-Freigabekreise
    - Grundgeräte 3TK2850-53
    - Erweiterungsgeräte 3TK2856-57
  - Motorschützkontakt-Freigabekreise
    - Grundgeräte 3RA710/1
    - Erweiterungsgeräte 3RA712-4
- mittlere Funktionalität
  - Multifunktionsgeräte 3TK2845

Aufbau

Die SIRIUS Sicherheitsschaltgeräte ohne integrierte Hilfsschütze werden in zwei kompakten Gehäusen im SIRIUS-Design (22,5 und 45 mm Baubreite) angeboten. Die elektronischen Sicherheitsschaltgeräte mit integrierten Hilfsschützen sowie die sicheren Verbraucherabzweige weisen eine Baubreite von 90 mm auf.

Alle Geräte sind für Schnappbefestigung auf einer Hutschiene 35 mm nach EN 50022 ausgeführt. Eine Schraubbefestigung der Gehäuse in Baubreite 22,5 und 45 mm ist mit zusätzlichen Einstecklaschen ebenso möglich. Hierzu werden die Einstecklaschen als Zubehör unter der Bestellnummer 3RP1903 angeboten.

Die Anschlussleitungen werden von oben und unten in die Geräte eingeführt. Die Schraubklemmen bzw. die Federzugklemmen sind von der Gerätefront aus zugänglich. Dieses ermöglicht eine einfache und übersichtliche Montage der Geräte. Die Klemmenblöcke der Geräte sind abnehmbar. Auf diese Weise lassen sich Anlagenstillstandszeiten im Servicefall auf ein Minimum reduzieren.

Funktionen

SIRIUS Sicherheitsschaltgeräte werden zum Auswerten von Sicherheitssensoren und zum Überwachen von Sicherheitsfunktionen verwendet.

Gemäß den Anforderungen der Normen müssen die Geräte sicherstellen, dass

a) Fehler im Sicherheitsschaltgerät oder im Sensor- / Aktorkreis rechtzeitig erkannt werden, um einen Verlust der Sicherheitsfunktion zu verhindern.

b) die Sicherheitsfunktion immer erhalten bleibt, auch wenn Fehler auftreten.

Um die oben beschriebenen Forderungen zu erfüllen, unterscheidet sich ein Sicherheitsschaltgerät in einigen wesentlichen Punkten von einem nicht sicherheitsgerichteten Schaltgerät.

Grundgerät/Basisgerät

Überwachung des Sensorkreises

Sensoren werden vom Sicherheitsschaltgerät auf Querschluss (2-kanaliger Anschluss) und verschweißte Kontakte überwacht. Dieses geschieht je nachdem, ob es sich um ein elektronisches oder ein Relaisgerät handelt, auf unterschiedliche Weise.

Querschluss: Beim Relaisgerät wird durch den Querschluss das P-Potential am Relais vorbei an Masse gelegt, dadurch fällt das Relais ab, und die Gefahr wird abgeschaltet. Bei der elektronischen Variante werden die elektromechanischen Sensoren durch elektronische Impulse überwacht. Stimmen die empfangenen mit den gesendeten Impulsen nicht überein, schaltet das Gerät ab.

Verschweißter Sensorkontakt:
Bevor das Gerät eingeschaltet werden kann, müssen beide Sensoreingänge bei 2-kanaligem Anschluss einmal geöffnet worden sein, sonst schaltet das Gerät nicht ein.

Überwachung des Aktorkreises

Externe Schütze, die den Laststromkreis der gefährlichen Bewegung schalten, werden ebenfalls vom Sicherheitsschaltgerät überwacht. Das Gerät hat Eingänge für den Anschluss von Rückmeldekontakten des Schützes. Sind die Kontakte nicht geschlossen, lässt sich das Sicherheitsgerät nicht einschalten. Die vom Gerät angesteuerten Schütze sind mit zwangsgeführten Kontakten versehen. Das Schütz hat Last- und Meldekontakte, die nicht gleichzeitig geschlossen sein können. Durch diese Funktion wird sichergestellt, dass sich das Sicherheitsgerät beim Verschweißen eines Lastkontaktes nicht mehr einschalten lässt.

Überwachung der eigenen Funktion

Durch die redundante Auslegung des "Innenlebens" des Schaltgerätes und die gegenseitige Überwachung der Funktionen führt ein Fehler in einem Bauteil zum Abschalten der gefährlichen Bewegung. In die Relaisgeräte sind zwei Sicherheitsrelais redundant eingebaut, die ihre Funktion gegenseitig überwachen. Die elektronischen Geräte sind mit zwei Microcontrollern versehen, die ihre Funktion gegenseitig überwachen. Bei einem Fehler in einem Microcontroller schaltet das Gerät die gefahrbringende Bewegung ab. Auf diese Weise bleibt selbst bei einem Fehler des Gerätes die Sicherheitsfunktion erhalten.

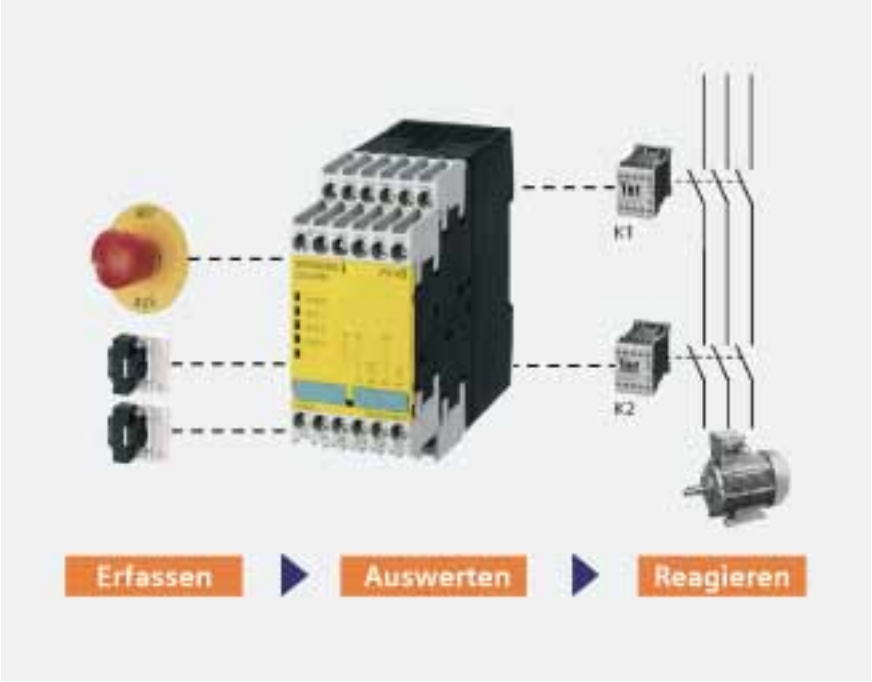
Fehler des Gerätes bzw. Betriebszustände werden durch eine LED an der Frontseite signalisiert.

Sicherheitsschaltgeräte werden überwiegend zur Realisierung von Sicherheitsfunktionen in Anlagen mit geringer räumlicher Ausdehnung ohne Anbindung an ein Bussystem (Inselbetrieb) verwendet. Die Geräte werden immer in einer sogenannten Sicherheitskette eingesetzt. Eine Sicherheitskette setzt sich aus den Funktionen ERFASSEN, AUSWERTEN und REAGIEREN zusammen.

Erfassen: Erkennen einer Sicherheitsanforderung, z.B. Betätigung eines Not-Halt oder Öffnen einer Schutztür durch einen Sensor.

Auswerten: Auswertung des Signals von Sensor und Überwachung der gesamten Sicherheitsfunktion durch das Sicherheitsschaltgerät.

Reagieren: Abschalten einer gefährlichen Bewegung



Erweiterungsgerät

Sollte die Anzahl der am Grundgerät vorhandenen sicherheitsgerichteten Freigabekreise für die Sicherheitsapplikation nicht ausreichen, kann sie durch ein Erweiterungsgerät erhöht werden (Kontaktvervielfacher). Ein Erweiterungsgerät besitzt nur diesen sicherheitsgerichteten Eingang, der über einen sicherheitsgerichteten Ausgang des Grundgerätes angesteuert wird. Über den Rückmeldekontakt des Erweiterungsgerätes überwacht das Grundgerät die Funktion des Erweiterungsgerätes. Erweiterungsgeräte dürfen nur in Verbindung mit Grundgeräten verwendet werden und erreichen die gleiche Sicherheitskategorie wie das Grundgerät.

Pressensteuergerät

Pressen gehören mit zu den gefährlichsten Verarbeitungsmaschinen. Um den Bediener, z.B. vor irreversiblen Verletzungen zu schützen, wird er durch das Zweihandbedienpult gezwungen, zum Betreiben beide Hände außerhalb des Gefahrenbereiches zu halten.

Die Auswertung des Zweihandbediengerätes übernimmt das Pressensteuergerät 3TK2834.

Das Gerät deckt folgende Fehler auf:

- Kurzschluss, z.B. zwischen den Tastern
- Defekte Relaisspulen
- Leiterbruch
- Verschweißte Kontakte

Die Freigabekreise können nicht zugeschaltet werden, wenn

- die Gleichzeitigkeit der beiden Drucktaster($\leq$ 0,5 s) nicht eingehalten wird
- nur ein Taster betätigt wird
- der Rückführkreis offen ist

Integration

Die Sicherheitsschaltgeräte 3TK28 / 3RA71 sind Bestandteil des Systems Safety Integrated. Die Geräte werden bevorzugt im Inselbetrieb eingesetzt, d.h. es ist keine Busanbindung notwendig. Über die Meldeausgänge können je nach verwendetem Gerätetyp sowohl Betriebszustände, als auch Diagnosedaten an eine übergeordnete Steuerung gemeldet werden.

Um die Sicherheitsfunktionen für komplexere Anlagen realisieren zu können, bzw. bereits bestehende Anlagen zu erweitern, sind die Sicherheitsschaltgeräte kaskadierbar (UND-Logik). Das bedeutet, die Geräte können miteinander verschaltet werden. Auf diese Weise lässt sich z.B. die Anzahl der sicheren Ausgänge vervielfachen (mit Erweiterungsblöcken), oder auch Abschaltgruppen bilden (selektives Abschalten).

Damit die oben beschriebene Sicherheitskette funktionieren kann, müssen an das Sicherheitsschaltgerät für die Funktionen ERFASSEN und REAGIEREN Sensoren und Aktoren angeschlossen werden.

Bei den Sensoren unterscheidet man zwischen kontaktbehafteten und elektronischen Sensoren.

Kontaktbehaftete Sensoren sind z.B.

- Not-Halt-Befehlsgeräte
- Scharnierschalter
- Positionsschalter
- Seilzugschalter
- Trittmatten
- usw.

Berührungslos wirkende Schutzeinrichtungen (BWS) mit Halbleiterausgängen sind z.B.

- Lichtschranken
- Lichtvorhänge/-gitter
- Laserscanner
- usw.

Als Aktoren werden z.B. die Schütze aus dem SIRIUS-Systembaukasten eingesetzt. Bei den Geräten der Baureihen 3TK285 und 3RA71 sind diese Hilfsschütze oder Lastschütze bereits integriert worden.

Der Einsatz dieser Geräte bietet zwei entscheidene Vorteile:

1. weniger Verdrahtungskosten durch werkseitige Vorverdrahtung

2. weniger mögliche Fehlerquellen bei der Vorort Verdrahtung und Montage

SIRIUS Sicherheitsschaltgeräte lassen sich nahtlos in das Konzept von Totally Integrated Automation (TIA) einbinden. Von der übergeordneten Anlagensteuerung (z.B. SPS) lassen sich die Schaltgeräte mit dem Kaskadiereingang oder über den Eingang für betriebsmäßiges Schalten direkt ansteuern. Dadurch ist ein betriebsmäßiges Schalten möglich, d.h. es sind keine zusätzlichen Schaltgeräte zum Schalten des Verbrauchers notwendig. Die Sicherheitsfunktion ist dem betriebsmäßigen Schalten immer übergeordnet.

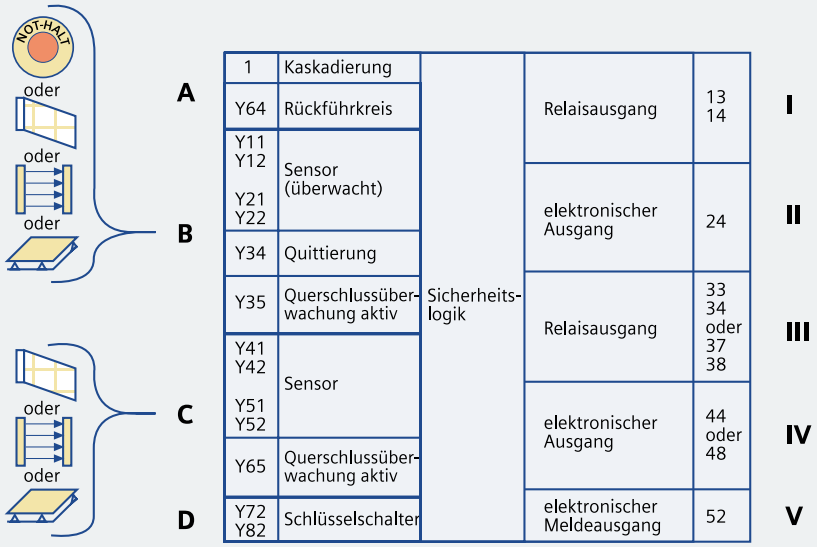
Beispiele

Anwendungsfall:

Eine Bearbeitungsmaschine ist mit einer Schutztür und einer Not-Halt Funktion versehen. In regelmäßigen Abständen muss das Bearbeitungswerkzeug der Maschine gegen ein Neues ausgetauscht werden. Dazu muss die Schutztür geöffnet werden. Über einen Schlüsselschalter kann zwischen Wartungsbetrieb und Normalbetrieb umgeschaltet werden.

Die Funktion wird mit einem 3TK2845 realisiert.

Bild 5/1
3TK2845

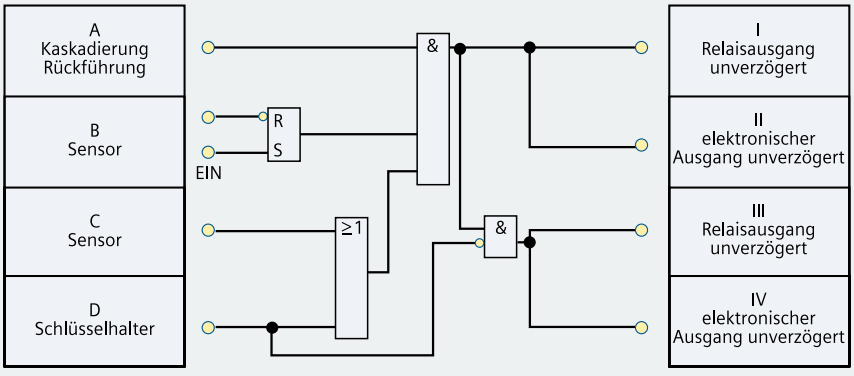


A	1	Kaskadierung	Sicherheitslogik	Relaisausgang	13 14 I
	Y64	Rückführkreis			
B	Y11 Y12 Y21 Y22	Sensor (überwacht)		elektronischer Ausgang	24 II
	Y34	Quittierung			
	Y35	Querschlussüberwachung aktiv		Relaisausgang	33 34 oder 37 38 III
C	Y41 Y42 Y51 Y52	Sensor		elektronischer Ausgang	44 oder 48 IV
	Y65	Querschlussüberwachung aktiv			
D	Y72 Y82	Schlüsselschalter		elektronischer Meldeausgang	52 V

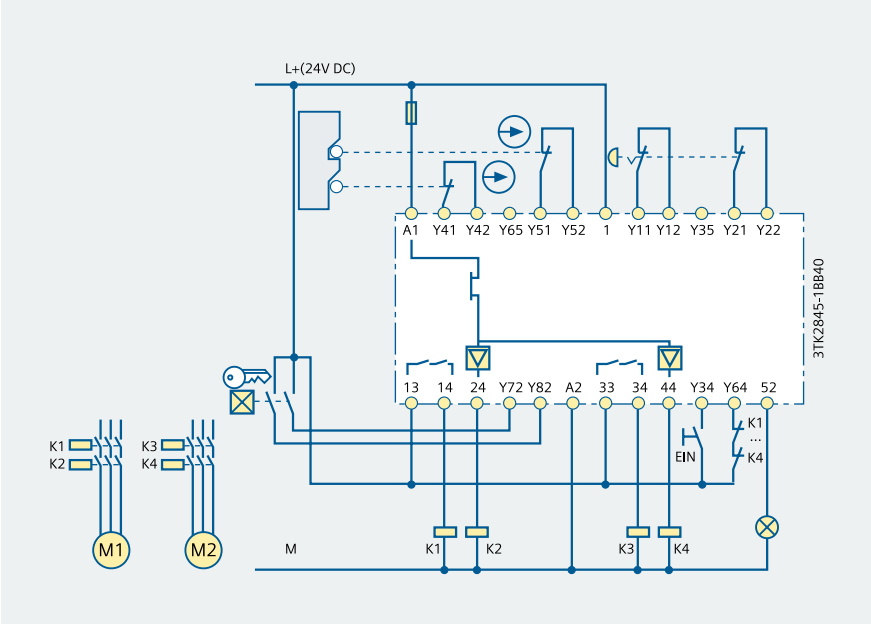
Normalbetrieb: Öffnen der Schutztür oder Betätigung des Not-Halt schalten alle Ausgänge des Auswertegerätes ab.

Wartungsbetrieb: Über denSchlüsselschalter wird nur die gefährliche Bewegung abgeschaltet. Die Nebenaggregate laufen weiter. Das Öffnen der Schutztür bewirkt keine Abschaltung aller Ausgänge mehr. Betätigung des Not-Halt schaltet weiterhin alle Ausgänge ab.

Sicherheitslogik



Schaltungsbeispiel



Normalbetrieb:

Bei Not-Halt- bzw. Schutztürbetätigung schalten die Ausgänge 14, 24 (M1), 34, 44 (M2) ab. Ein Wiedereinschalten der Anlage ist erst möglich, wenn Not-Halt entriegelt ist, die Schutztüre und der Rückführkreis (RF) an Y64 geschlossen sind. Nach Not-Halt Betätigung muss zusätzlich der EIN-Taster an Y34 gedrückt werden. Die Ausgänge schalten sich nach dem Schließen der Schutztür automatisch wieder ein.

Schlüsselschalter betätigen (Servicebetrieb aktivieren):
Die Ausgänge 34, 44 (M2) schalten ab (für Ansteuerung einer Drehzahlreduzierung geeignet oder Antriebsteile sind nicht in Betrieb).

Servicebetrieb:

Die Positionsschalter der Schutztüre werden nicht ausgewertet. Die Ausgänge 34 und 44 (M2) sind aus.

Bei Betätigen des Not-Halt schalten auch die Ausgänge 14 und 24 (M1) ab.

Ein Wiedereinschalten der Anlage ist erst möglich, wenn Not-Halt entriegelt ist, der Rückführkreis an Y64 geschlossen ist und der EIN Taster Y34 gedrückt wird.

Bemerkung:
Für Kat. 4 ist die Reihenschaltung mehrerer Positionsschalter für Schutztürüberwachung nicht erlaubt (Fehleraufdeckung).

		Sichere Ausgänge					
	max. Kategorie	Kontakte		elektronisch		Meldekreis	
	nach EN 954-1	Stop-Kat. 0	Stop-Kat. 1	Stop-Kat. 0	Stop-Kat. 1	Kontakt	elektronisch
Einfache Funktionalität (1 Sicherheitssensor anschließbar)							
eketronische Freigabekreise							
unverzögerte, sichere Ausgänge							
3TK2840-.BB40 Basisgerät	3	--	--	2	--	--	--
3TK2841-.BB40 Standardgerät	4	--	--	2	--	--	--
verzögerte, sichere Ausgänge							
3TK2842-.BB4. Standardgerät mit Zeitverzögerung 3s - 300s	4	--	--	1	1	--	--
Relaiskontakt-Freigabekreise							
unverzögerte, sichere Ausgänge							
3TK2821-.CB30 Grundgerät Autostart	3	3	--	--	--	1	--
3TK2822-.CB30 Grundgerät Autostart	4	2	--	--	--	--	--
3TK2824-..... Grundgerät Autostart	4	2	--	--	--	--	--
3TK2825-..... Grundgerät Autostart	4	3	--	--	--	2	--
3TK2823-.CB30 Grundgerät automatischer Start	4	2	--	--	--	--	--
3TK2830-..... Erweiterungsgerät	wie Grundgerät	4	--	--	--	--	--
3TK2834-..... Zweihand-Steuergerät	4	2S + 2Ö	--	--	--	--	--
3TK2835-..... Nachlaufweg-Prüfgerät	--	3S + 1Ö	--	--	--	--	--
verzögerte, sichere Ausgänge							
3TK2828-..... Grundgerät Autostart mit Zeitverzögerung 0.5 - 30s, 0.05 - 3s	4	2	2	--	--	1	--
3TK2827-..... Grundgerät überwachter Start mit Zeitverzögerung 0.5 - 30s, 0.05 - 3s	4	2	2	--	--	1	--
Hilfsschütz-Freigabekreise							
unverzögerte, sichere Ausgänge							
3TK2850-..... Grundgerät	3	3	--	--	--	--	--
3TK2851-..... Grundgerät	3	2	--	--	--	1	--
3TK2852-..... Grundgerät	3	6	--	--	--	1	--
3TK2853-.BB40 Grundgerät	3	3	--	--	--	--	--
3TK2856-.BB40 Erweiterungsgerät unverzögert	wie Grundgerät	6	--	1	--	1	--
verzögerte, sichere Ausgänge							
3TK2857-.BB4. Erweiterungsgerät mit Zeitverzögerung 3s - 300s	wie Grundgerät	--	3	1	--	--	--
Leistungsschütz-Freigabekreise							
unverzögerte, sichere Ausgänge							
3RA710 Grundgerät bis Kategorie 3	3	3	--	--	--	*	--
3RA711 Grundgerät bis Kategorie 4	4	3	--	--	--	*	--
3RA712 Erweiterungsgerät unverzögert	wie Grundgerät	3	--	--	--	*	--
verzögerte, sichere Ausgänge							
3RA713 Erweiterungsgerät mit Zeitverzögerung 0.05 - 3 s	wie Grundgerät	--	3	--	--	*	--
3RA714 Erweiterungsgerät mit Zeitverzögerung 0.5 - 30 s	wie Grundgerät	--	3	--	--	*	--
Mittlere Funktionalität (2 Sicherheitssensoren anschließbar)							
elektronische und Relaiskontakt-Freigabekreise							
unverzögerte, sichere Ausgänge							
3TK2845-.BB40 Multifunktionsgerät unverzögert	4	2	--	2	--	--	1
verzögerte, sichere Ausgänge							
3TK2845-.BB4. Multifunktionsgerät mit Zeitverzögerung 0.05 - 300s	4	1	1	1	1	--	1

* durch aufgesetzte Hilfsschalter möglich

Weitere technische Details befinden sich im Katalog sowie in den technischen Dokumentationen im Internet unter:
http://www.siemens.de/automation/service

	Bemessungssteuerspeisespannung / V	Betriebsbemessungsspannung / V	Schaltvermögen				elektronische Sensoren	Gehäusebreite / mm
			AC-1	AC-3	AC-15	DC-13		
			bei Ue=400V, 50Hz	bei Ue=400V, 50Hz	bei U=230 V	bei U= 24 V		
	24 V	24 V	--	--	--	0,5 A	nein	22,5
	24 V	24 V	--	--	--	1,5 A	ja	22,5
	24 V	24 V	--	--	--	1,5 A	ja	22,5
	AC/DC 24 V	DC 24 V - AC 230 V	--	--	5 A	5 A	nein	22,5
	AC/DC 24 V	DC 24 V - AC 230 V	--	--	5 A	5 A	nein	22,5
	AC/DC 24 V, DC 24 V, AC 115 V, AC 230 V	DC 24 V - AC 230 V	--	--	5 A	5 A	nein	22,5
	AC/DC 24 V, DC 24 V, AC 115 V, AC 230 V	DC 24 V - AC 230 V	--	--	6 A	6 A	nein	45
	AC/DC 24 V	DC 24 V - AC 230 V	--	--	5 A	5 A	nein	22,5
	AC/DC 24 V, AC 115 V, AC 230 V	DC 24 V - AC 230 V	--	--	5 A	5 A	nein	45
	DC 24 V, AC 24 V, AC 115 V, AC 230 V	DC 24 V - AC 230 V	--	--	6 A	6 A	nein	45
	DC 24 V, AC 24 V, AC 115 V, AC 230 V	DC 24 V - AC 230 V	--	--	5 A	5 A	nein	45
	DC 24 V, AC 24 V, AC 115 V, AC 230 V	DC 24 V - AC 230 V	--	--	5 A	5 A	nein	45
	DC 24 V, AC 24 V, AC 115 V, AC 230 V	DC 24 V, AC 230 V, AC 600 V	--	--	6 A	10 A	nein	90
	DC 24 V, AC 24 V, AC 115 V, AC 230 V	DC 24 V, AC 230 V, AC 600 V	--	--	6 A	10 A	nein	90
	DC 24 V, AC 230 V	DC 24 V, AC 230 V, AC 600 V	--	--	6 A	10 A	nein	90
	DC 24 V	DC 24 V, AC 230 V, AC 600 V	--	--	6 A	10 A	nein	90
	DC 24 V	DC 24 V, AC 230 V, AC 600 V	--	--	6 A	10 A	--	90
	DC 24 V	DC 24 V, AC 230 V, AC 600 V	--	--	6 A	10 A	--	90
	AC 690 V	DC 24 V, AC 230 V			--	--	nein	90
	AC 690 V	DC 24 V, AC 230 V			--	--	ja	90
	AC 690 V	DC 24 V, AC 230 V			--	--	--	90
	AC 690 V	DC 24 V, AC 230 V			--	--	--	90
	AC 690 V	DC 24 V, AC 230 V			--	--	--	90
	24 V	24 V, 230 V	--	--	2 A	1,5 A	ja	45
	24 V	24 V, 230 V	--	--	2 A	1,5 A	ja	45

5.5 ASIsafe

Verweis - Anknüpfung

Übersicht, Merkmale / Kundennutzen sowie Funktion / Aufbau und Anwendungsbereiche wurden in Kap 4.2 (Sichere Kommunikation über Standard-Feldbusse; Abschnitt ASIsafe) erläutert.

Im Folgenden wird daran anknüpfend das Produktspektrum im einzelnen aufgeführt und ein Beispielaufbau gezeigt.

Sicherheitsmonitore

Der Sicherheitsmonitor ist das Kernstück von ASIsafe. Die Konfiguration einer sicheren Applikation erfolgt mit einem PC. Hierbei können verschiedene anwendungsspezifische Betriebsmodi ausgewählt werden.
Dies sind z.B. Not-Halt-Funktion, Schutztürzuhaltung sowie die Auswahl von Stop-Kategorie 0 oder 1. Um die ASI Diagnosemöglichkeiten voll ausschöpfen zu können, kann der Monitor wahlweise auch mit AS-Interface-Adresse betrieben werden. Es gibt zwei Varianten des Monitors:

- Basis Sicherheitsmonitor
- Erweiterter Sicherheitsmonitor

Beide Ausbaustufen sind jeweils mit einem oder zwei zweikanalig ausgeführten Freigabekreisen erhältlich.

SIRIUS Not-Halt

Über den Standard ASI-Interface mit sicherheitsgerichteter Kommunikation können Not-Halt-Geräte direkt angebunden werden.
Dies gilt für Not-Halt-Geräte der Befehlsgeräte SIRIUS 3SB3 für Frontplatteneinbau und für Einbau in einem Gehäuse. Ein in eine Frontplatte eingebauter Not-Halt kann über ein sicheres Modul direkt am AS-Interface angebunden werden.

Not-Halt in Kapselungen

Unterschiedliche Gehäuse mit 3SB3-Befehlsgeräten können mit Not-Halt direkt am ASIsafe angebunden weden.
Auch kundenspezifische Anordnung der Befehls- und Meldegeräte innerhalb der Gehäuse bestellbar.

SIRIUS Positionsschalter

Über das Standard AS-Interface mit sicherheitsgerichteter Kommunikation können auch SIRIUS Positionsschalter direkt angebunden werden. Hierfür gibt es eine Direktanbindung, die an das Gewinde eines Positionsschalters montiert wird. Die Komponenten für die Sicherheitsfunktionen müssen daher nicht mehr konventionell verdrahtet werden.

SIGUARD Lichtvorhänge und Lichtgitter

Die Lichtvorhänge und Lichtgitter der Kategorie 4 nach EN 954-1 bieten aktiven optischen Schutz für Personen an Maschinen. Sie können direkt und sicherheitsgerichtet am AS-Interface direkt angebunden werden.

SIGUARD Laserscanner LS4

Der Laserscanner ist eine optische, berührungslos wirkende Schutzeinrichtung zur Gefahrbereichsabsicherung bis zu einem Radius von 4 m. Die AS-Interface Variante erlaubt einen direkten sicherheitsgerichteten Anschluss.

Sicheres Modul K45F

Das sichere Kompaktmodul K45F ist mit 2 sicherheitsgerichteten Eingängen für elektromechanische Geber ausgestattet.
Im Betrieb bis Kategorie 2 nach EN 954-1 können beide Eingänge separat verwendet werden. Ist Kategorie 4 erforderlich, steht am Modul ein 2-kanaliger Eingang zur Verfügung.

Sicheres Modul K60F

Das sichere Kompaktmodul K60F ist mit 2 sicherheitsgerichteten Eingängen für elektromechanische Geber ausgestattet.
Im Betrieb bis Kategorie 2 nach EN 954-1 können beide Eingänge separat verwendet werden, ist Kategorie 4 erforderlich, steht am Modul ein 2-kanaliger Eingang zur Verfügung. Zusätzlich sind am Modul zwei nicht sicherheitsgerichtete Ausgänge vorhanden. K60F gibt es in zwei Varianten:

- Spannungsversorgung der Ausgänge über das gelbe Kabel
- Hilfsspannungsversorgung der Ausgänge über das schwarze Kabel(U_{hilf})

Sicheres Modul S22,5F

Das sichere SlimLine Modul S22,5F ist mit 2 „sicheren" Eingängen für elektromechanische Geber ausgestattet und ermöglicht die Einbindung sicherer Signale an ASIsafe in die dezentralen Vor-Ort-Schaltkästen und Schaltschränken.
Im Betrieb Kategorie 2 können beide Eingänge separat belegt werden. Ist Kategorie 4 erforderlich, steht am Modul ein 2-kanaliger Eingang zur Verfügung

Alle wichtigen Normen und Vorschriften werden erfüllt, z.B.:

- IEC 61508 (bis SIL 3),
- EN 954 (bis Kategorie 4)

Technische Daten

Es gibt zwei Varianten des Sicherheitsmonitors:

- Basis Sicherheitsmonitor
- Erweiterter Sicherheitsmonitor

Beide Ausbaustufen sind jeweils mit einem oder zwei zweikanalig ausgeführten Freischaltkreisen erhältlich.

Tabelle: Vergleich Basis Sicherheitsmonitor – Erweiterter Sicherheitsmonitor

	Basis Sicherheitsmonitor	Erweiterter Sicherheitsmonitor
Anzahl Überwachungsbausteine	32	48
Anzahl Oder-Gatter (Eingänge)	2	6
Anzahl Und-Gatter (Eingänge)	-	6
Platzhalter für Überwachungsbausteine	ja	ja
Deaktivieren von Überwachungsbausteinen	ja	ja
Fehlerentriegelung	ja	ja
Diagnose halt	ja	ja
A/B- Slaves zur Quittierung	ja	ja
Sichere Zeitfunktionen	nein	ja
Funktion „Taste"	nein	ja
Entprellen von Kontakten	nein	ja

	Sicherheitsmonitor
	3RK1 105
Bemessungsbetriebsstrom	
• I_e/AC-12	bis 250 V, 3 A
• I_e/AC-15	115 V, 3 A 230 V, 3 A
• I_e/DC-12	bis 24 V, 3 A
• I_e/DC-13	24 V, 1 A 115 V, 0,1 A 230 V, 0,05 A
• Ansprechzeit (worst case) in ms	≤40
• Umgebungstemperatur in °C	0 ... +60
• Lagertemperatur in °C	-40 ... +85

Beispiel Verpackungsmaschine

Die folgende Abbildung zeigt eine typische Anwendung von ASIsafe:

Beschreibung des Ablaufs:

Leere Kartons werden über das Förderband 1 zur Befüllung antransportiert. Das Füllgut wird über das Förderband 3 zum Roboter befördert.
Dieser befüllt die leeren Kartons. Anschließend werden die befüllten Kartons über das Förderband 2 abtransportiert.

Schutzeinrichtungen:

Um das Personal vor Verletzungen zu schützen, wird der Roboter mit einem Schutzzaun umgeben.
Die Lichtgitter sorgen für ein Abschalten der Applikation innerhalb des Schutzzauns.
Der Seilzugschalter ermöglicht das Abschalten des Förderbands 1.
Der Not-Halt schaltet die gesamte Anlage sicherheitsgerichtet ab.
Zu Wartungszwecken ist eine Tür im Zaun vorgesehen. Diese wird über eine Schutztürzuhaltung überwacht. Bei Betreten der Anlage über die Tür wird die Applikation innerhalb des Schutzzauns abgeschalten.

Realisierung mit ASIsafe:

Die nebenstehende Abbildung zeigt die Beschaltung einer AS-Interface Lösung.
Der Sicherheitsmonitor 1 schaltet die Leistung des Motors 1.
Der Sicherheitsmonitor 2 schaltet die Leistung des Motors 2 und 3.

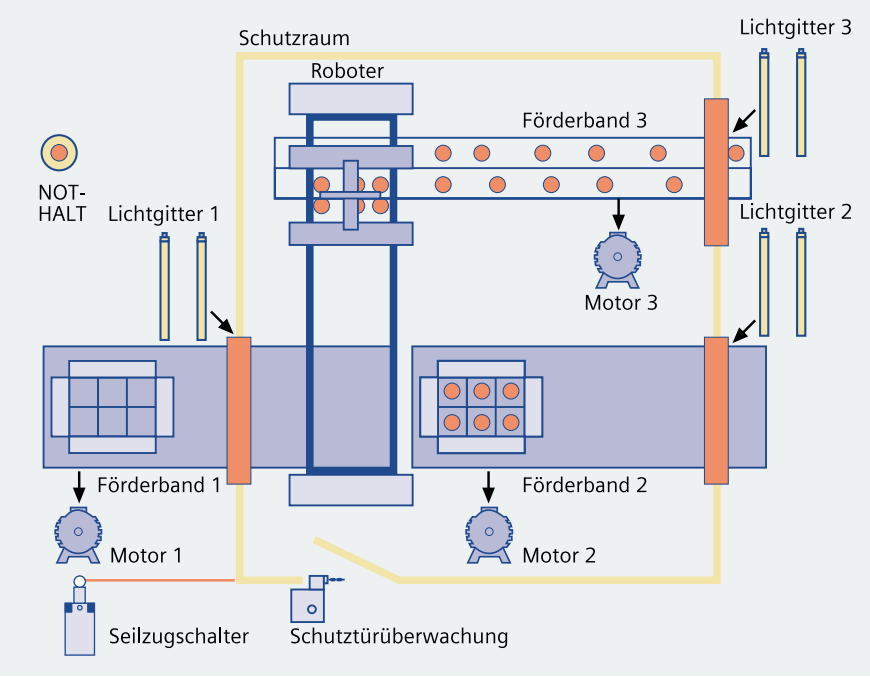


Bild 5/2
Kombination von sicheren Slaves am Beispiel einer Verpackungsmaschine. Zeigt auch die gezielte, sichere Abschaltung von Teilbereichen.

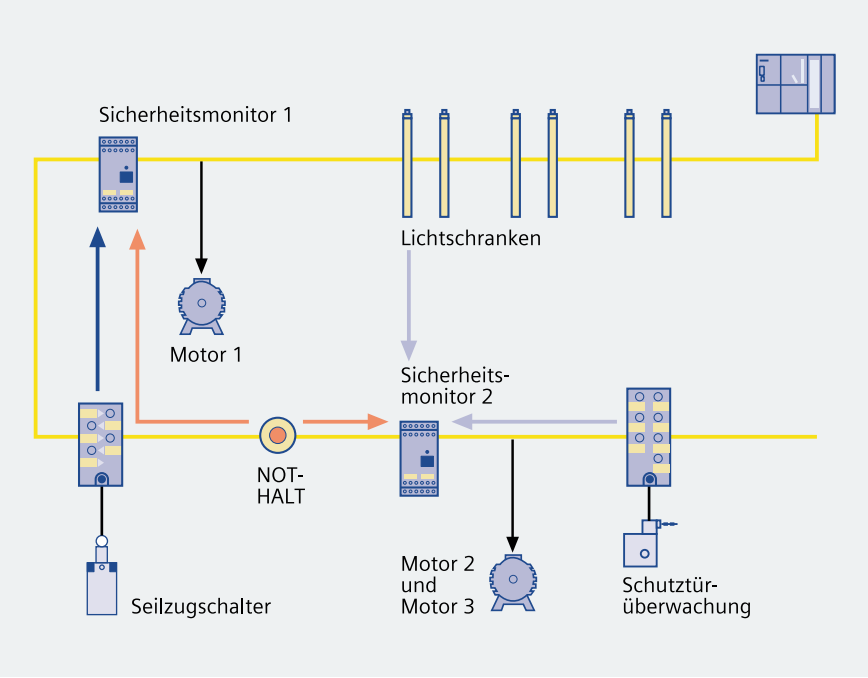


Bild 5/3
Gruppenbildung mit ASIsafe

ASIsafe ermöglicht die Gruppierung sicherer Signale.
Dabei können die sicheren Slaves den Sicherheitsmonitoren zugeordnet werden. Die Schutztürüberwachung und die Lichtschranken werden dem Sicherheitsmonitor 2 zugewiesen (hellblaue Pfeile).
Der Seilzugschalter wird dem Sicherheitsmonitor 1 zugewiesen (blauer Pfeil). Der Not-Halt-Schalter wird beiden Sicherheitsmonitoren zugewiesen (rote Pfeile).

Somit schaltet der Seilzugschalter über ein sicheres Modul den Sicherheitsmonitor 1 ab.
Die Lichtschranken und die Schutztür schalten die Applikation innerhalb des Schutzzauns über den Sicherheitsmonitor 2 ab.

Die gesamte Anlage kann über den Not-Halt abgeschaltet werden, der beiden Sicherheitsmonitoren zugeordnet ist.

5.6 ET 200S Safety Motorstarter Solution

Übersicht

Die ET 200S Safety Motorstarter Solutions bestehen aus:

- Safety Modulen
- ET 200S Motorstarter Standard
- ET 200S Motorstarter High Feature
- ET 200S Motorstarter Failsafe

Die Geräte sind ausgelegt für den Einsatz im dezentralen Peripheriesystem ET 200S. Die Motorstarter sind mit galvanisch trennenden Schaltelementen ausgestattet.

Diese Safety Motorstarter Solutions können beliebige Drehstromverbraucher sicherungslos schützen und schalten. Alle notwendigen Ein- und Ausgänge zur Einbindung der Motorstarter und Sicherheitstechnik in die übergeordnete Steuerung sind bereits integriert. Durch die Kommunikationsschnittstelle und die umfangreichen Diagnosemöglichkeiten sind sie auch optimal für den Einsatz in dezentralen Schaltschränken (Schutzart IP20) geeignet.

Bei den ET 200S Safety Motorstarter Solutions entfällt der aufwändige und somit kostenintensive Projektierungs- und -verdrahtungsaufwand im Vergleich zur konventioneller Sicherheitstechnik. Die ET 200S Safety Motorstarter Solutions sind für die Kategorie 4 nach EN 954-1 bzw. SIL 3 (IEC 61508) ausgelegt.

Anwendungsbereich

Die ET 200S Motorstarter Solutions werden bevorzugt in allen Branchen der Fertigungs- und Prozessautomatisierung, in denen die Reduzierung der Fertigungszeiten oder die Erhöhung der Anlagenverfügbarkeit eine große Rolle spielen, eingesetzt.

1. ET 200S Motorstarter Solution Local sind aus Sicht der Sicherheitstechnik bevorzugt auf eine Station beschränkt.

2. ET 200S Motorstarter Solution PROFIsafe sind dagegen häufig in miteinander vernetzten und komplexeren Sicherheitstechnikanwendungen zu finden.

Technische Erfordernisse

- PROFIBUS oder PROFINET
  Wird die ET 200S Safety Motorstarter Solution PROFIsafe gewünscht, sind zusätzlich eine sicherheitsgerichtete Steuerung SIMATIC und als Kommunikationsmedium PROFIBUS oder PROFINET mit dem PROFIsafe Profil erforderlich.

Kundenanforderungen

- Einfache Integration in die Standardautomatisierung von sicheren Direkt- oder Reversierstartern bis 7,5 kW / bei 500 V nach DIN VDE 0106, Teil 1014 – IEC 60947-1, EN 60947-1 und bei 600 V nach UL, CSA.
- Durchgängiges Gesamtsystem und komplette Sicherheitstechnik aus einer Hand.
- Erleichterung der Projektierung dank durchgängiger Tools.

- Einfache Anbindung von sicherheitsgerichteten Komponenten wie z.B. Not-Halt-Befehlsgeräte, Schutztürüberwachungsgeräte oder Lichtvorhänge via Safety Module.
- Bei komplexen Anforderungen an die Sicherheitstechnik eine kostengünstige Lösung im Vergleich zu konventioneller Technik mit Verbraucherabzweigen und diskreter Sicherheitstechnik.
- Reduzierter Prüf- und Dokumentationsaufwand.
- Schneller Aufbau und Inbetriebnahme
- Erweiterbarkeit einer Anlage mit weniger Projektierungs- und Verdrahtungsaufwand.
- Hohe Verfügbarkeit durch umfangreiche Diagnose (schnelle Fehlerbehebung) und Wartungsfreundlichkeit (einsteckbare Modulen / Hot Swapping) * .

Merkmale

Die ET 200S Safety Motorstarter Solutions ermöglichen die Anwendung von sicherheitsgerichteten Direkt- oder Reversierstartern im dezentralen Peripheriesystem SIMATIC ET 200S. Durch die feinmodulare Architektur des Systems können die Applikationen von Maschinen oder Anlagen optimal abgebildet werden.

Die Motorstarter sind geeignet zum Schalten und Schützen von Drehstromverbrauchern.
Motorstarter Standard: max. 5,5 kW (AC 500 V) mit selbstaufbauenden Energiebus bis 40 A

Motorstarter High Feature: max. 7,5 kW (AC 500 V) mit selbstaufbauendem Energiebus bis 50 A
Motorstarter Failsafe: max. 7,5 kW (AC 500 V) mit selbstaufbauendem Energiebus bis 50 A
Alle Motorstarter können optional erweitert werden mit Modulen zum Ansteuern von motorintegrierten Bremsen.

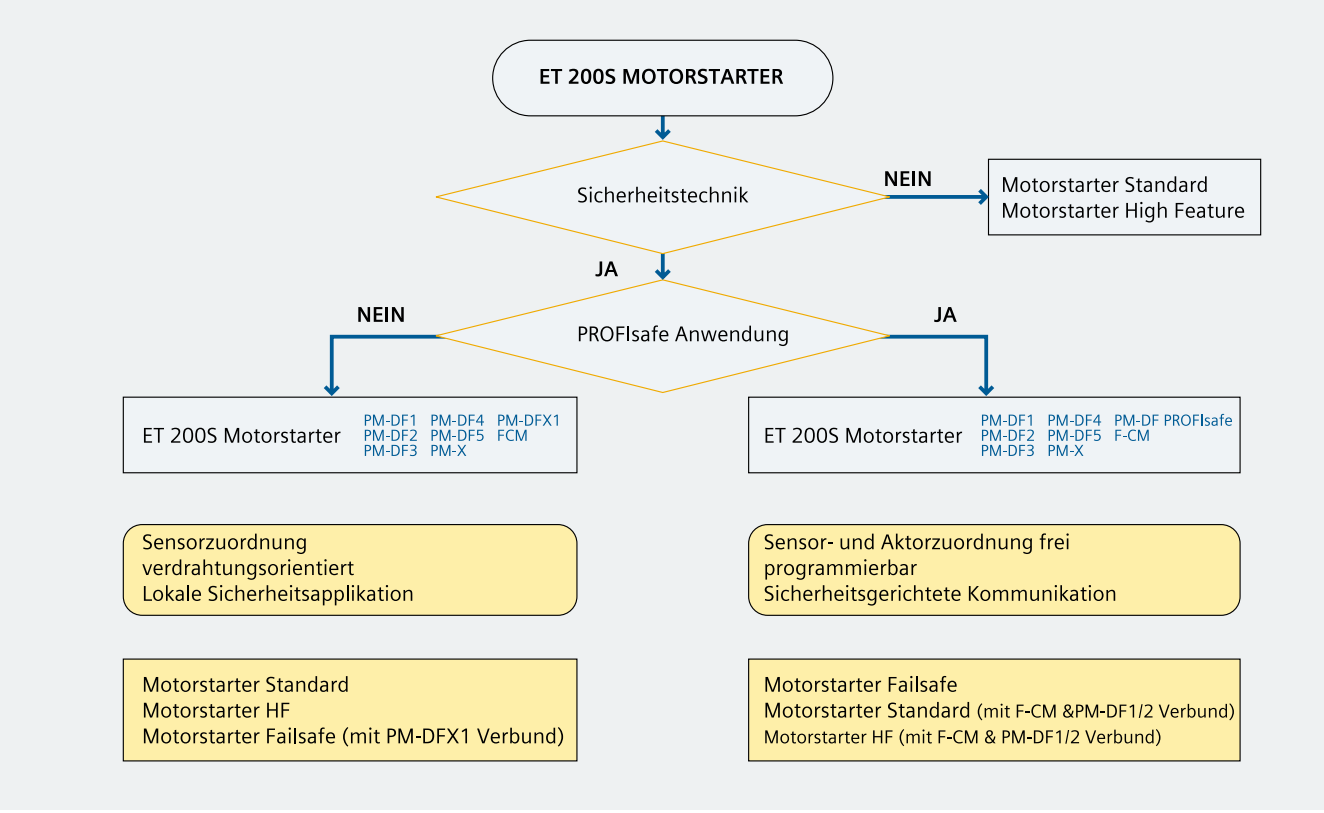


Bild 5/4
ET 200S Motorstarter

* Hot swapping: Gerätetausch im laufenden Betrieb ohne Folgen für die laufende CPU bzw. Motorstarter.

Die ET 200S Safety Motorstarter Solutions sind innerhalb einer ET 200S Station auch mit den Frequenzumrichtern SIMATIC ET 200S FC kombinierbar (siehe Kap. 9.3). Auch hier können sicherheitsgerichtete Komponenten mit nicht sicherheitsgerichteten Komponenten kombiniert werden.

Das gesamte System SIMATIC ET 200S ist UL/CSA approbiert.
Die ET 200S Motorstarter Failsafe sind vom TÜV zertifiziert.

ET 200S Safety Motorstarter Solution Local Verdrahtungsorientierte Sensorzuordnung: Die Logik der Sicherheitsfunktionen wird mit Hilfe der Verdrahtung realisiert

Mit ET 200S Safety Motorstarter Solution Local lassen sich problemlos mehrere Sicherheitskreise aufbauen. Die Sicherheitssensorik wird direkt an den Safety Modulen angeschlossen. Diese Safety Module übernehmen die Aufgabe der sonst obligatorischen Sicherheitsrelais und Schalten in Abhängigkeit der jeweils gewählten Funktion die nachfolgenden Motorstarter sicher ab. Die dazu benötigten Querverbindungen sind im System bereits integriert und bedürfen keiner Zusatzverdrahtung. Selbstverständlich lassen sich ET 200S Motorstarter auch in Verbindung mit externen Sicherheitsrelais oder mit ASIsafe einsetzen.

Mit der ET 200S Safety Motorstarter Solution Local wird in Vergleich zu konventionellen Sicherheitstechnik bei lokalen Sicherheitsapplikationen viel Verdrahtung eingespart.

Es gibt drei Varianten:

Lokale Sicherheitsapplikationen ET 200S Motorstarter Standard: Gruppenabschaltung

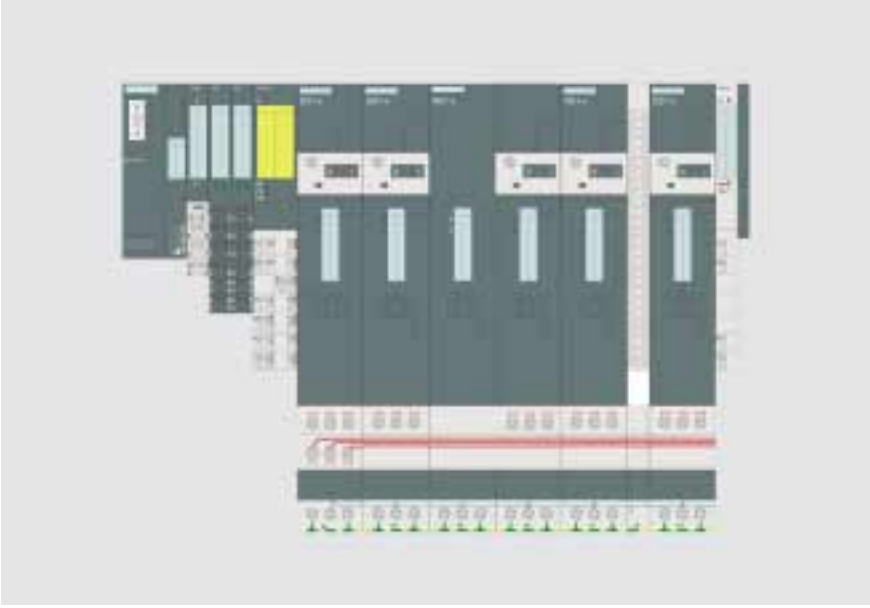


Bild 5/5
ET 200S Safety Motorstarter Solution Local (mit Motorstarter Standard) F-Kits 1 oder 2 notwendig. Ab Kat. 3 EN 954-1: Redundant schaltendes, externes Einspeiseschütz nötig

Bild 5/6
Dezentraler Schaltkasten mit ET 200S Safety Motorstarter Solution Local

- Schnelle, gleichzeitige Zusammenfassung in einem dezentralen Peripheriesystem von mehreren überwachten Motorstartern bis 5,5 kW zu einer oder mehreren Sicherheitsgruppen. Deshalb können auch komplexere sicherheitstechnische Anwendungen mit der ET 200S Safety Motorstarter Solution Local abgedeckt werden (bis zu 42 Motorstarter Standard können in einer einzigen Station kombiniert werden).

Da die ET 200S Safety Motorstarter Solution für den Einsatz bis Kategorie 4 gemäß EN 954-1 optimiert ist, werden Defekte vom System erkannt und ein Wiedereinschalten nach einer Sicherheitsabschaltung wird verhindert. Diese Aufgaben übernehmen die Safety Module PM-DF1 / PM-DF2 / PM-DF3 / PM-X.

Verschiedene Funktionen sind möglich:

- Not-Halt Abschaltung (PM-D F1 Safety Modul / überwachter Start) Schutztürüberwachung (PM-D F2 Safety Modul / automatischen Start) Erweiterung von Sicherheitskreisen mit anderen Motorstartern, z.B. in einer anderen Zeile (PM-D F4) Zeitverzögerte Abschaltung (STOP 1 durch PM-D F3) Sichere Kontaktvervielfachung (PM-D F5)
- Einsetzbar in Verbindung mit externen Sicherheitskreisen. Integration in bisherige Sicherheitskonzepte möglich.
- Einfache Diagnosemöglichkeit: Störungen in der Anlage werden automatisch und ohne Programmieraufwand über Bus gemeldet.
- Selbstbauender 40 A Energiebus
- Für Anwendungen mit wenig Änderungsbedarf bzw. Flexibilität bei der Zuordnung der Sicherheitssegmente empfohlen.

Lokale Sicherheitsapplikationen mit ET 200S Motorstarter High Feature: Gruppenabschaltung

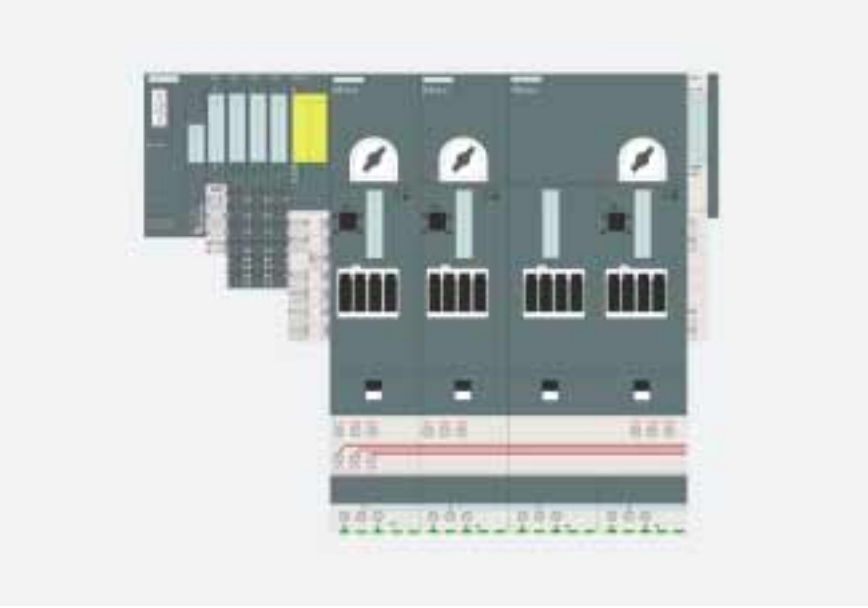


Bild 5/7
ET 200S Safety Motorstarter Solution Local (mit Motorstarter High Feature)
Die Motorstarter HF und deren Terminalmodule haben die Funktion der F-Kits bereits serienmäßig integriert. Ab Kat. 3 EN 954-1: Redundant schaltendes, externes Einspeiseschütz nötig.

Die Motorstarter Standard und die Motorstarter High Feature können auch beliebig miteinander kombiniert werden und z.B. zu einer einzigen Abschaltgruppe zusammengefasst werden.

Gegenüber dem Motorstarter Standard hat der Motorstarter High Feature weitere Vorteile:

- Motorstarter bis 7,5 kW mit nur zwei Varianten (Weiteinstellbereich)
- Zuordnungsart Typ 2
- Wird der Motorstarter High Feature angewendet, unterscheidet das selektives Schutzkonzept zwischen Überlast und Kurzschluss. So kann eine Überlastauslösung über den Bus fernquittiert werden.
- Parametrierung via PROFIBUS.
- Bei Austausch (unter Spannung zulässig!) erfolgt automatischer Download aller Parameterdaten von der überlagerten SPS.
- Bis zu 29 Motorstarter High Feature in einer Station (max. 2 m Breite).
- Selbstbauender 50 A Energiebus
- Umfangreiche Diagnose bei den Motorstartern, z.B. Stromgrenzwert
- Statistikdaten, z.B. Strom der letzten Überlastauslösung oder Anzahl Schaltspiele, können zu Service oder Inbetriebnahmezwecken mit der Software Switch ES Motorstarter ausgelesen werden.

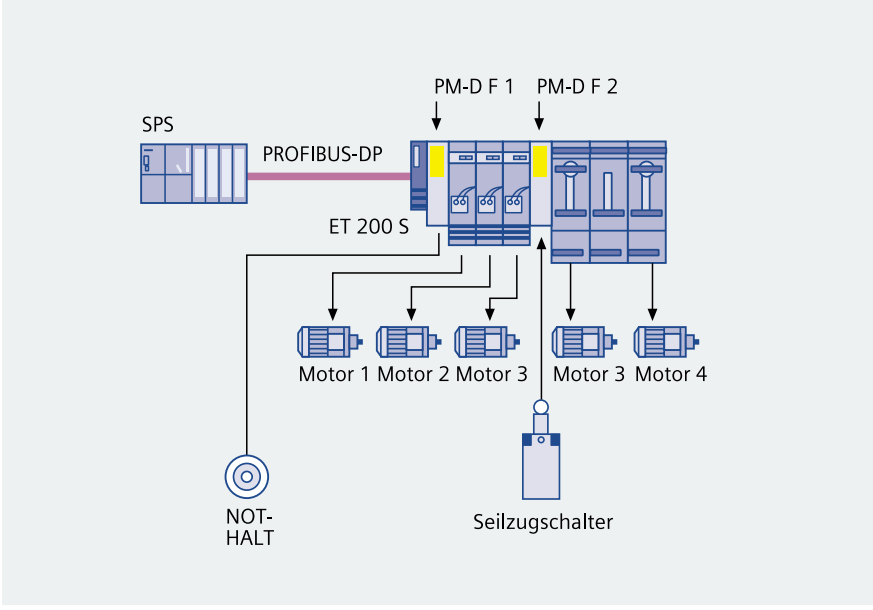


Bild 5/8
ET 200S Safety Motorstarter Solution Local mit Motorstartern Failsafe (PM-D F1, PM-D F2 Anwendung)

Lokale Sicherheitsapplikationen mit Motorstartern Failsafe: Selektive Abschaltung.

Bild 5/9
ET 200S Safety Motorstarter Solution Local (mit Motorstarter Failsafe und PM-D FX1) Als redundantes zweites Abschaltelement wird kein externes Einspeiseschütz, sondern der Leistungsschalter des Motors verwendet.

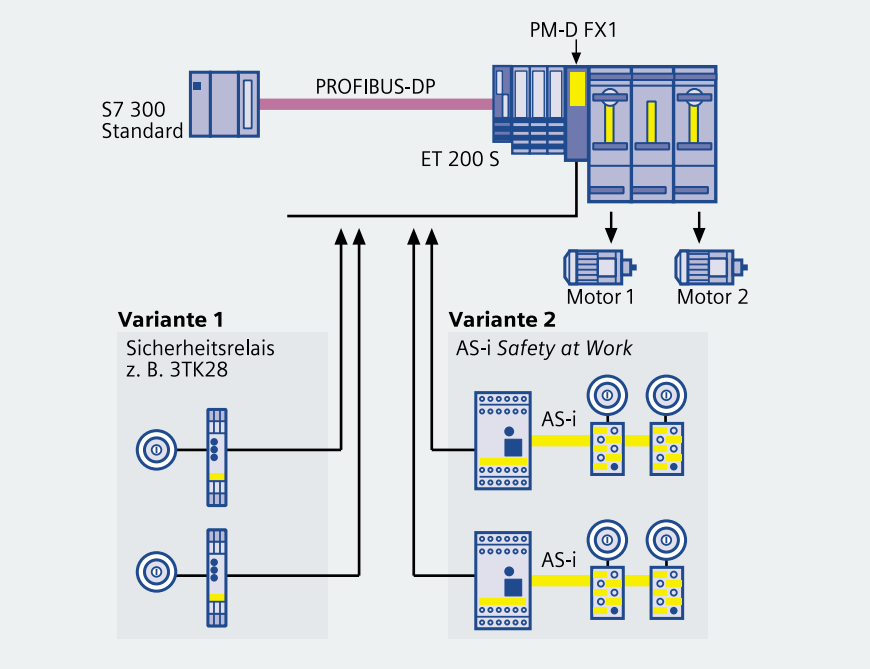


Bild 5/10
ET 200S Safety Motorstarter Solution Local mit Motorstartern Standard und High Feature

Im Rahmen der ET 200S Safety Motorstarter Solution Local (ohne F-CPU bzw. ohne PROFIsafe Kommunikation) hat eine Kombination mit Motorstarter Failsafe zusätzlich folgende Kundennutzen:

- Die Motorstarter Failsafe können in Verbindung mit Sicherheitsrelais oder mit ASIsafe eingesetzt werden. Durch die Freigabe eines ASIsafe Sicherheitsmonitors oder eines Sicherheitsschaltgerätes können sicherheitsgerichtete Signale über das Einspeisemodul PM-D FX1 in die ET 200S Station eingespeist und somit die Motorstarter Failsafe angesteuert werden, die dann die Motoren sicher abschalten.

- Die externen Sicherheitsgeräte können aus der sicheren Spannung U1 vom PM-D FX1 aus versorgt werden.

- Vollselektive Sicherheitsabschaltung: Ein Safety Modul PM-D FX1 kann in Summe 6 Sicherheitsabschaltgruppen durch den Zugriff auf die 6 Schienen SG1 bis SG6 (Safety groups) bedienen. Es leitet die gesicherte Steuerspannung der Abschaltgruppen SG1 bis 6 auf die Potenzialschienen der Terminalmodule bis hin zu den nachfolgenden Motorstartern Failsafe. Terminalmodule der Motorstarter Failsafe haben zusätzlich einen Kodierbaustein, der die Zuordnung des Motorstarters auf eine der sechs Abschaltgruppen ermöglicht. Die Abschaltung erfolgt, indem ein externer ASIsafe-Sicherheitsmonitor oder ein Sicherheitsschaltgerät jeweils eine der 6 SGx-Schiene spannungslos schaltet.

- Die sicherheitsgerichtete Abschaltung des Motorstarters Failsafe erfolgt durch dessen Schütz. Durch eine integrierte Auswertelektronik zur Fehlererkennung schaltet bei Versagen des Schützes der Leistungsschalter zusätzlich ab. Eine spezifische Diagnosemeldung meldet einen solchen Fehlerfall automatisch an die übergeordnete Steuerung. Die redundante Abschaltung erfolgt nur bei einem Fehler in einem Motorstarter Failsafe.

- Deutlich weniger Hardware benötigt: Schütze, Hilfsschalter, Zusatzmodule sind nicht mehr notwendig. Dadurch deutliche Einsparung von Verdrahtung.

- Es können bis zu 29 Motorstarter Failsafe in einer Station (2 m max.) eingebaut werden.

- Motorstarter Failsafe bis 7,5 kW mit mehr Diagnose: Einzelschalteridentifizierung, Querschluss, Schützversagen. Statusanzeige pro sicherheitsgerichteter Abschaltgruppe

- Das Safety Modul PM-D FX1 stellt einen Weiterleitungsknoten dar. Die sicherheitsgerichtete Potenzialgruppe kann mit einer oder mehreren ET 200S Stationen gekoppelt werden.

- Die ET 200S Safety Motorstarter Solution Local mit PM-D FX1 kann mit dem Safety Modul F-CM erweitert werden. Das Safety Modul F-CM stellt 4 sichere potenzialfreie Relaiskontakte zur Verfügung, über die weitere Aktoren oder Geräte sicher abgeschaltet werden können.

- Ein wichtiger Nutzen des Kontaktvervielfachers F-CMs ist die sicherheitsgerichtete Ansteuerung eines separaten, großen Schützes, wenn Motoren

die maximale Leistung der ET 200S Motorstarter (> 7,5 kW) überschreiten. Die Ansteuerung des F-CM erfolgt mittels eines Safety Moduls PM-D FX1.

ET 200S Safety Motorstarter Solution PROFIsafe
Sensor- und Aktorzuordnung sind im Rahmen des Distributed Safety Konzeptes frei programmierbar: Jede Sicherheitsfunktion lässt sich hiermit realisieren.

Kommt eine sicherheitsgerichtete SIMATIC CPU zum Einsatz, steht die ET 200S als sicherheitsgerichtete Peripherie zur Verfügung. Trotzdem können in einer solchen Station Motorstarter und Ein-/Ausgabemodule in konventioneller Technik mit Modulen mit Sicherheitsfunktionen gemischt aufgebaut werden.

Da die Safety Funktionen im gesamten Netzwerk verfügbar sind, ermöglicht die ET 200S Safety Motorstarter Solution PROFIsafe die selektive Abschaltung einer Gruppe von Motorstartern Standard, High Feature oder Motorstartern Failsafe, egal wo und an welcher Peripheriestation die sicheren Befehlsgeräte angeschlossen wurden. So bietet diese Lösung eine bisher nicht gekannte Flexibilität und Verdrahtungsreduzierung für Anwendungen in räumlich ausgedehnten Anlagen bzw. mit sporadischem Änderungsbedarf bei der Zuordnung der Sicherheitssegmente. Die ET 200S Motorstarter Solution PROFIsafe ist optimal für Sicherheitskonzepte mit Kat. 2 bis 4 gemäß EN 954-1, SIL 2 und 3 gemäß IEC 61508 geeignet.

Es gibt drei Varianten:

Sicherheitsapplikationen mit sicherheitsgerichteter Kommunikation und Motorstarter Standard: Gruppenabschaltung

Das Safety Modul F-CM (Kontaktvervielfacher) ist eine wichtige Ergänzung der fehlersicheren Peripheriebaugruppen der ET 200S, um eine Schnittstelle von der ET 200S Station zu Anlagen mit konventioneller Sicherheitstechnik wie z.B. Robotern darzustellen.

Es ist auf eine sicheren Abschaltgruppen SG1 bis SG6 eines Safety Moduls PM-D F PROFIsafe zuordenbar und besteht aus vier getrennten potenzialfreien Freigabekreisen als Schließer. Bei jedem EIN – AUS Zyklus des Kontaktvervielfachers werden die Schaltglieder des F-CM auf korrektes Öffnen und Schließen überprüft. Ein neuer Start des Gerätes wird durch die Zwangsführung der Kontakte verhindert, wenn verschweißte Kontakte in beliebigen Freigabekreisen vom F-CM erkannt worden sind. Eine entsprechende Diagnosemeldung wird in diesem Fall an die übergeordnete Steuerung weitergegeben.

Das Safety Modul F-CM bildet eine Schnittstelle zwischen einer PROFIsafe Applikation zu einer verdrahtungsorientierten Motorstartergruppe. So können Motorstarter Standard verwendet und über PROFIsafe sicher abgeschaltet werden.

- Kostengünstige Realisierung bei einer Abschaltgruppe
- Einbindung eines redundant schaltenden, externen Einspeiseschütz über das Safety Modul PM-X (nur bei Kat. 3 oder 4 EN 954-1 nötig)
- Überwachung des Rückführkreises über PM-D F2
- Motorschutz bis 5,5 kW durch Leistungsschalter
- Verhalten bei CPU STOP einstellbar
- Sammeldiagnose

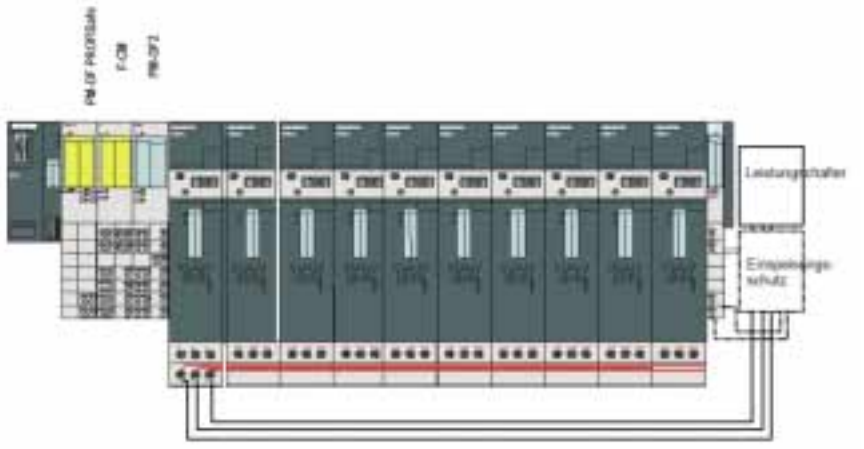


Bild 5/11
ET 200S Safety Motorstarter Solution PROFIsafe (mit Motorstarter Standard) zusätzlich F-Kits 1 oder 2 notwendig. Ab Kat. 3 EN 954-1: Redundant schaltendes, externes Einspeiseschütz nötig

Sicherheitsapplikationen mit sicherheitsgerichteter Kommunikation und Motorstarter High Feature: Gruppenabschaltung

Gegenüber den Motorstarter Standard haben die Motorstarter High Feature folgende Vorteile:

- Rückführkreis bereits integriert (kein F-Kit notwendig)
- Elektronischer Motorschutz bis 7,5 kW
  Verhalten bei Überlast thermisches Motormodell
  Verhalten bei Stromgrenzwertverletzung
  Verhalten bei Nullstromerkennung
  Verhalten bei Unsymmetrie
  Verhalten bei CPU STOP
- Fernreset nach Überlastauslösung möglich
- Sammeldiagnose
- Erweiterte Einzeldiagnose

Bild 5/12
ET 200S Safety Motorstarter Solution PROFISAFE (mit Motorstarter High Feature)
F-Kits 1 und 2 überflüssig: Die Motorstarter High Feature und deren Terminalmodule haben die Funktion der F-Kits serienmäßig eingebaut. Ab Kat. 3 EN 954-1:Redundant schaltendes, externes Einspeiseschütz nötig

Sicherheitsapplikationen mit sicherheitsgerichteter Kommunikation und mit Motorstartern Failsafe: Vollselektive Abschaltung

Innerhalb einer ET 200S Station werden die Motorstarter auf eines von sechs Sicherheitssegmenten zugeordnet. Bei dezentral aufgebauten Anlagen erfolgen die Abschaltsignale dieser Sicherheitssegmente vorzugsweise von einer übergeordneten sicherheitsgerichteten Steuerung via PROFIsafe. Damit verbunden ist die höchstmögliche Flexibilität bei der Zuordnung der Motorstarter zu unterschiedlichen Sicherheitskreisen. Alternativ kann aber auch mit einem ET 200S Interfacemodul mit sicherheitsgerichteter CPU angesteuert werden. Dies empfiehlt sich insbesondere bei lokal begrenzten Anwendungen und einfacheren Sicherheitsverknüpfungen. Die Ansteuerung von externen Sicherheitssystemen, wie z.B. AS-Interface ist ebenfalls möglich. Soll eine Station um weitere Abschaltgruppen erweitert werden, ist der PROFIsafe Aufbau mit den Motorstartern Failsafe kostengünstiger im Vergleich zur PM-D F1/2 Anwendung.

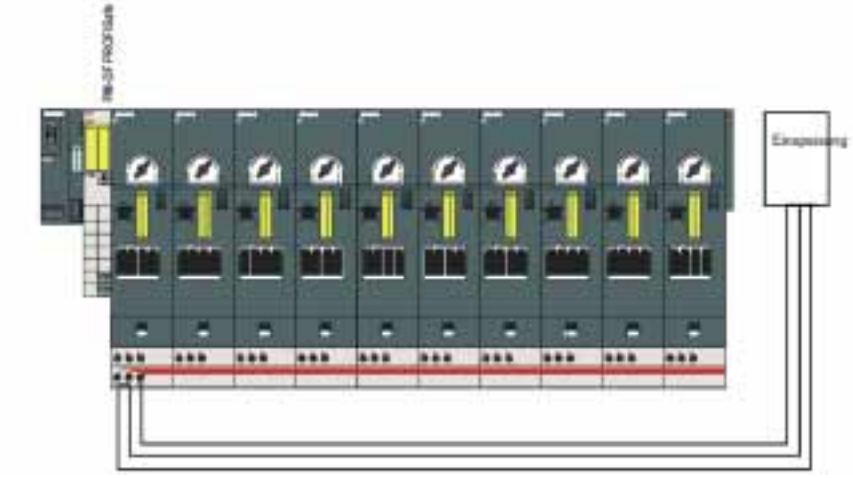


Bild 5/13
ET 200S Safety Motorstarter Solution PROFISAFE (mit Motorstarter High Feature)
F-Kits 1 und 2 überflüssig: Das redundante zweite Abschaltelement ist kein Hauptschütz mehr, sondern ein in den Motorstartern eingebauter Leistungsschalter mit Hilfsauslöser.

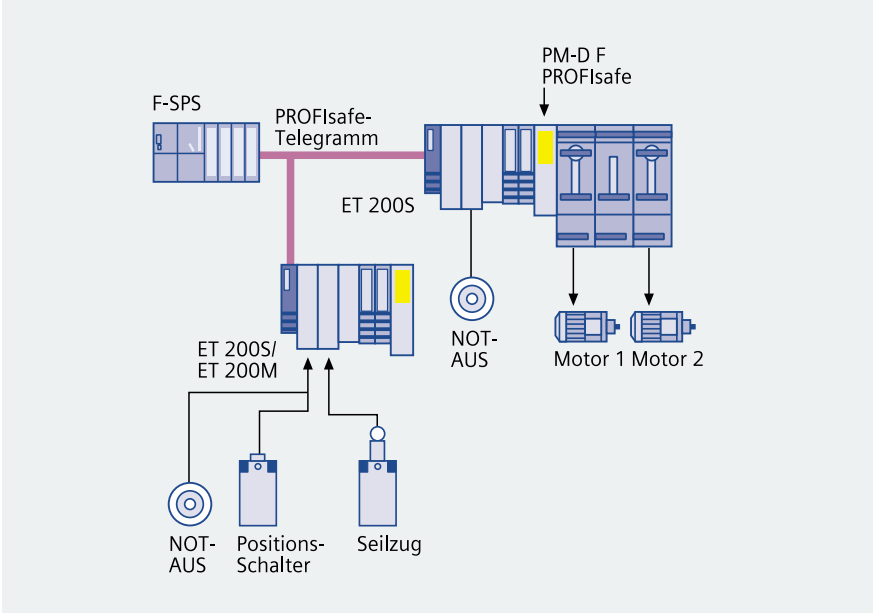


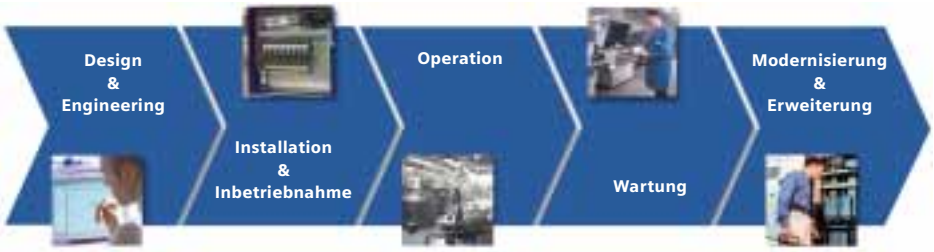
Bild 5/14
ET 200S Safety Motorstarter Solution PROFIsafe mit Motorstartern Failsafe (PM-D F PROFIsafe Anwendung)

Highlights: Fehlersicherheit pur

Die neuen Motorstarter Failsafe besitzen neben einer Leistungschalter-Schützkombination eine sichere elektronische Auswerteschaltung zur Fehlererkennung. Versagt im Not-Halt-Fall das zu schaltende Schütz, erkennt die integrierte Doppelprozessor-Überwachung einen Fehler, z.B. bei verschweißten Schützkontakten und schaltet den Leistungschalter im Motorstarter sicherheitsgerichtet ab. Somit erreicht jeder einzelne Motorstarter ohne zusätzliche Einspeiseschütze (Redundanzschütz) und Rückführkreis die Kat. 4 nach EN 954-1 bzw. SIL 3 nach IEC 61508.

Für sicherheitsgerichtete Anwendungen bringen die ET 200S Safety Motorstarter Solution über jede Phase eines Anlagen-Lebenszyklus durch ihre optimale Integration bei gleichzeitig hoher Flexibilität viele Vorteile für Anlagen- und Maschinenbauer sowie für Anlagenbetreiber:

„Industrial equipment Life Cycle"



Erfüllte Anforderungen	Anlagen- und Maschinenbauer	Anlagen-Betreiber	Merkmal
Phase 1: DESIGN und ENGINEERING			
Geringerer Aufwand für Projektierung und Dokumentation	✓		• Umparametrierung und Dokumentation der Motorstarter mit Standardwerkzeug STEP7 • Alle Steuerfunktionen der Motorstarter durch die SPS projektierbar • Vorgefertigte Programmierbeispiele für die Sicherheitsfunktionen • Weniger Komponenten: z.B. nur 2 Varianten von Motorstartern High Feature oder Failsafe bis 7,5 kW mit großen Einstellbereichen
Schnellere Reproduzierbarkeit	✓		Software-Lösung kann im Gegensatz zur Hardware-Lösung einfach vervielfältigt werden
Höhere Flexibilität	✓	✓	• Vollselektive sicherheitsgerichtete Sicherheitsabschaltung. • Die Logik der Sicherheitsfunktionen wird über Software realisiert – nicht mittels Verdrahtung
Phase 2: INSTALLATION und INBETRIEBNAHME			
Deutlich schnellere Montage	✓		• Optimaler Schaltschrankaufbau durch waagerechten „Dicht-an-dicht-Aufbau" der Motorstarter ohne Derating bis 60° C • Bis zu 90% weniger Steuer-/Sicherheits-Verdrahtung aufgrund der in ET 200S integrierten Sicherheitstechnik und der datentechnischen Kopplung mit S7-300F über PROFIsafe • Durch Schnellstmontagetechnik der ET 200S mit selbstaufbauendem Energiebus, Wegfall diverser Kabelkanäle, Ersatz von Reihenklemmen • Alle Versorgungsspannungen nur einmal angeschlossen und automatisch mit den nächsten Modulen verbunden. • Alle Motorstarter sind bis auf den Motorenanschluss komplett verdrahtet.
Geringerer Platzbedarf (wenig / kleinere Schaltschränke)	✓	✓	• Kompaktere Lösung • Bisher separate Komponenten entfallen wegen der integrierten Redundanz und der integrierten Safety-Überwachung
Deutlich schnellere Inbetriebnahme	✓		• Einfache Prüfung dank Standardisierung und modularem Anlagenkonzept • Deutlich weniger Verdrahtungsfehler möglich • Schnittstelle für Software Switch ES Motorstarter
Kostengünstigere und einfachere Abnahme (Maschinenrichtlinie)	✓	✓	Vom TÜV zertifizierte Motorstarter, Safety Module und Programmierbeispiele (F-Bibliothek)
Einkaufkostenreduzierung	✓		Die aufsteckbaren Motorstarter müssen oft erst Wochen später zur Verfügung stehen. So wird die Kapitalbindung reduziert.

Erfüllte Anforderungen	Anlagen- und Maschinenbauer	Anlagen-Betreiber	Merkmal
Phase 3: OPERATION			
Steigern die Verfügbarkeit und die Produktivität		✓	• Frühere Störungserkennung durch bessere Diagnosefunktionen • Sollen Motorstarter von Anlagen- oder Maschinenteilen bei Busunterbrechung verfügbar bleiben, kann die entsprechende Station mit Intelligenz vor Ort (IM151 CPU) projektiert werden. • Einfache Überlastquittierung der Motorstarter durch Fernreset über PROFIBUS • Im Überlastfall, bzw. bei Stromgrenzwertverletzung kann der Motorstarter auf Warnen, bzw. Abschalten parametriert werden. • Notstartfunktion • Zuordnungsart „2“ für 50 kA
Phase 4: WARTUNG			
umfangreiche Diagnose bei den Motoren		✓	• Getrennte Erfassung von Überlast und Kurzschluss mit Diagnosebaustein in STEP 7 • Die eindeutige Diagnose (Ermittlung der gestörten Komponente) muss nicht eigens programmiert (F-SPS) bzw. verdrahtet (Elektromechanik) werden
Kürzere Stillstandszeiten		✓	• Hot Swapping (werkzeugloser Austausch von Motorstartern unter Spannung in wenigen Sekunden), „stehende Verdrahtung“ und Selbstkodierung der Motorstarter (das Stecken falscher Motorstarter mechanisch wird verhindert). • Fernparametrierung automatisch durch den PROFIBUS Master bei Austausch unter Spannung. • Motorvollschutz durch Überlastschutz, Kurzschlussschutz, Unsymmetrie- und Blockierschutz (Motoranlaufklassen 10, 10A, 20) • Lange Lebensdauer von Motorstartern bis 10 Millionen Schaltspiele
Weniger Aufwand für Ersatzteilhaltung		✓	Weniger Komponenten für die Sicherheitsfunktionen (anstelle einer Vielzahl elektromechanischer Komponenten proportional zur Komplexität der F-Funktionen gibt es einige wenige Komponenten unabhängig von der Komplexität der F-Funktionen) und nur max. 2 Varianten von Motorstartern mit großen Einstellbereichen des Motornennstroms.
Einfache und planbare vorbeugende Wartung		✓	• Überwachung von Motornennströmen • Diagnose für Stromgrenzwertverletzung und Statistik
Phase 5: MODERNISIERUNG UND ERWEITERUNG			
Einfache Änderungsprojektierung	✓	✓	Software-Lösung mit Standardwerkzeug STEP7 und Parametrierung statt neuer Verdrahtung
Einfache Integration in bisherige Sicherheitskonzepte	✓	✓	Einsetzbar in Verbindung mit externen / konventionellen Sicherheitskreisen.
Einfacher Anschluss an nicht kommunikationsfähigen Anlagen	✓	✓	Mit Safety Modul FCM stehen sichere potenzialfreie Relaisausgänge zur Verfügung.

Anwendungsbereich

Die ET 200S Safety Motorstarter Solution Local wird in allen Anlagen eingesetzt, in denen:

- Drehstromverbraucher bis 7,5 kW geschützt und geschaltet werden sollen.
- Ein Peripheriesystem in Verbindung mit einer nicht sicherheitsgerichteten SPS in Schutzart IP20 mit PROFIBUS DP oder PROFInet Schnittstelle sinnvoll wird.
- Lokale Sicherheitstechnik in räumlich begrenzten Anlagen(-teilen) für sichere Verbraucherabschaltung gefordert wird.
- Keine F-CPU eingesetzt werden soll.

ET 200S Safety Motorstarter Solution PROFIsafe wird in allen Anlagen eingesetzt, in denen:

- Drehstromverbraucher bis 7,5 kW geschützt und geschaltet werden sollen.
- Ein Peripheriesystem in Verbindung mit einer sicherheitsgerichteten SPS mit PROFIBUS DP Schnittstelle sinnvoll wird.
- Eine sicherheitsgerichtete, kommunikationsfähige Verbraucherabschaltung gefordert wird.
- Optimal für den Einsatz in weiträumigen Anlagen

Diese Lösung ist für das Distributed Safety-Konzept prädestiniert.

Konfigurationsbeispiel

bestehend aus einer Steuerung mit Peripherie, Operator Panel, Laserscanner und Lichtvorhang.

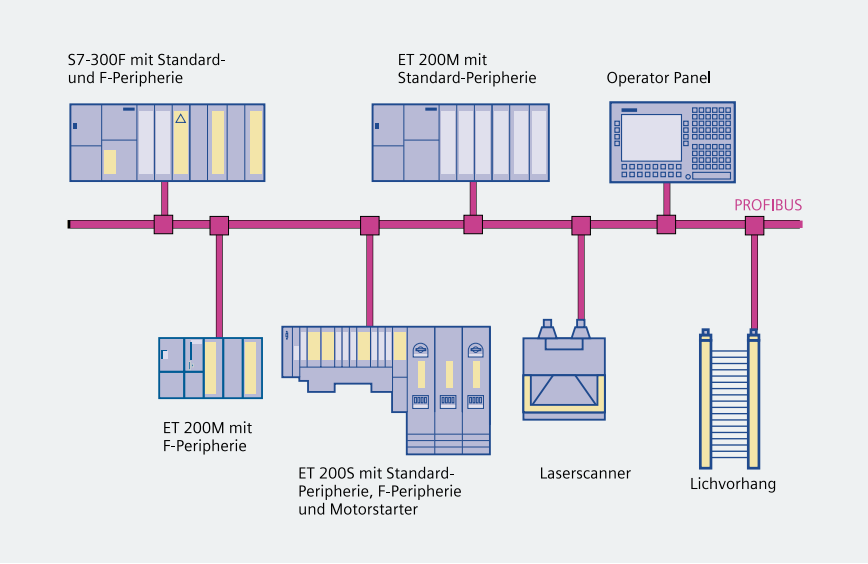


Bild 5/15

Einsatzgebiete für die ET 200S Safety Motorstarter (ohne oder mit PROFIsafe) Solution finden sich hauptsächlich in der Fertigungsindustrie aber auch in der Prozessindustrie.

Hier ein Beispiel für die Werkzeugmaschine in der Fertigungsindustrie:

- SINUMERIK/SIMODRIVE als PROFIsafe-Master
- 1 ET 200S Reversierstarter für den Revolverkopf
- 1 Direktstarter für die Werkzeugschmierpumpe
- Not-Halt- und Gefahrenbereich Überwachung

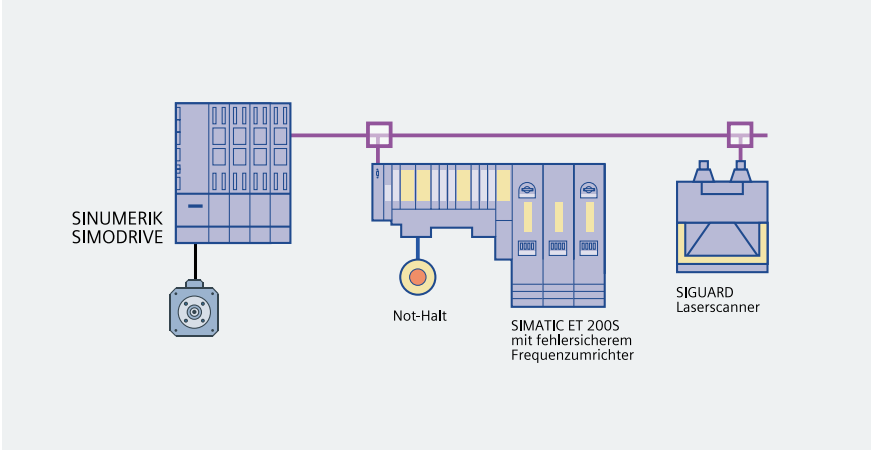


Bild 5/16
Applikationsbeispiel in der Fertigungsindustrie

Folgende Baugruppen stehen zur Verfügung:

PM-D F PROFIsafe

Sicherheitsgerichtetes Powermodul PROFIsafe mit 6 integrierten sicheren Abschaltschienen (SIL 3), 24 V und 2 A zur sicheren Abschaltung von nachgeordneten Motorstarter Failsafe oder Kontaktvervielfachern, bei interner Ansteuerung über PROFIsafe.

PM-D F X1

Sicherheitsgerichtetes Powermodul (Einspeiseklemmenmodul) mit 6 integrierten sicheren Abschaltschienen (SIL 3), 24 V und 2 A zur sicheren Abschaltung von nachgeordneten Motorstarter Failsafe oder Kontaktvervielfachern, bei Abschaltung durch externe Sicherheitsschaltgeräte mit potenzialfreien Kontakten (z.B. 3TK28, ASIsafe-Sicherheitsmonitor, Relaisausgängen von Sicherheits-SPSen, etc.).

F-CM

Sicherheitsgerichteter Kontaktvervielfacher mit 4 (SIL 3) Ausgängen für 24 V und 2 A

Motorstarter Failsafe

Sicherheitsgerichtete Direkt- und Reversierstarter bis 7,5 kW Schaltleistung, mit redundanter galvanischer Trennung

Ein ET 200S Konfigurator erlaubt die schnelle, einfache und richtige Konfiguration des dezentralen Peripheriesystems ET 200S.

Vorteile:

- Stücklisten und Bestelldaten werden automatisch generiert.
- Schnelle Vorabkalkulation.
- Übersichtliche grafische Darstellung.
- Automatische Konfigurations- und Aufbauprüfung.

Der ET 200S Konfigurator ist kostenlos auf der Katalog-CD-ROM CA01 und im Internet verfügbar.

Aufbau

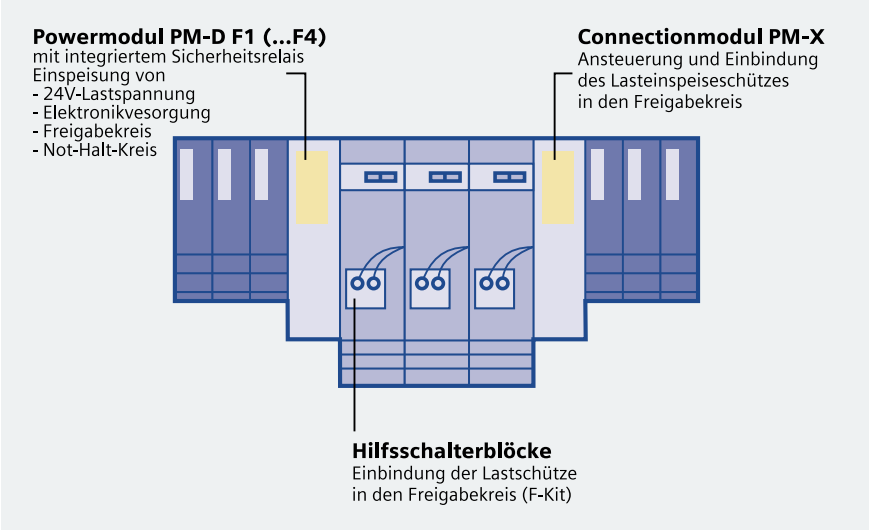


Bild 5/17
Aufbau einer ET 200S Safety Motorstarter Solution Local mit Motorstarter Standard und montierten F-Kits Station

Beispiele

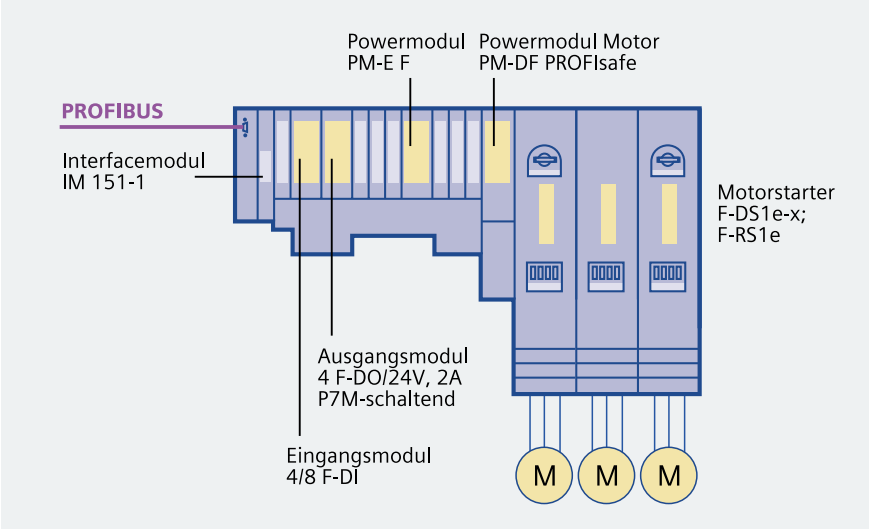


Bild 5/18
Aufbau einer ET 200S Safety Motorstarter Solution PROFIsafe mit Motorstarter Failsafe

Bild 5/19
Dezentraler Schaltschrank mit ET 200S Motorstarter Failsafe

Technische Daten

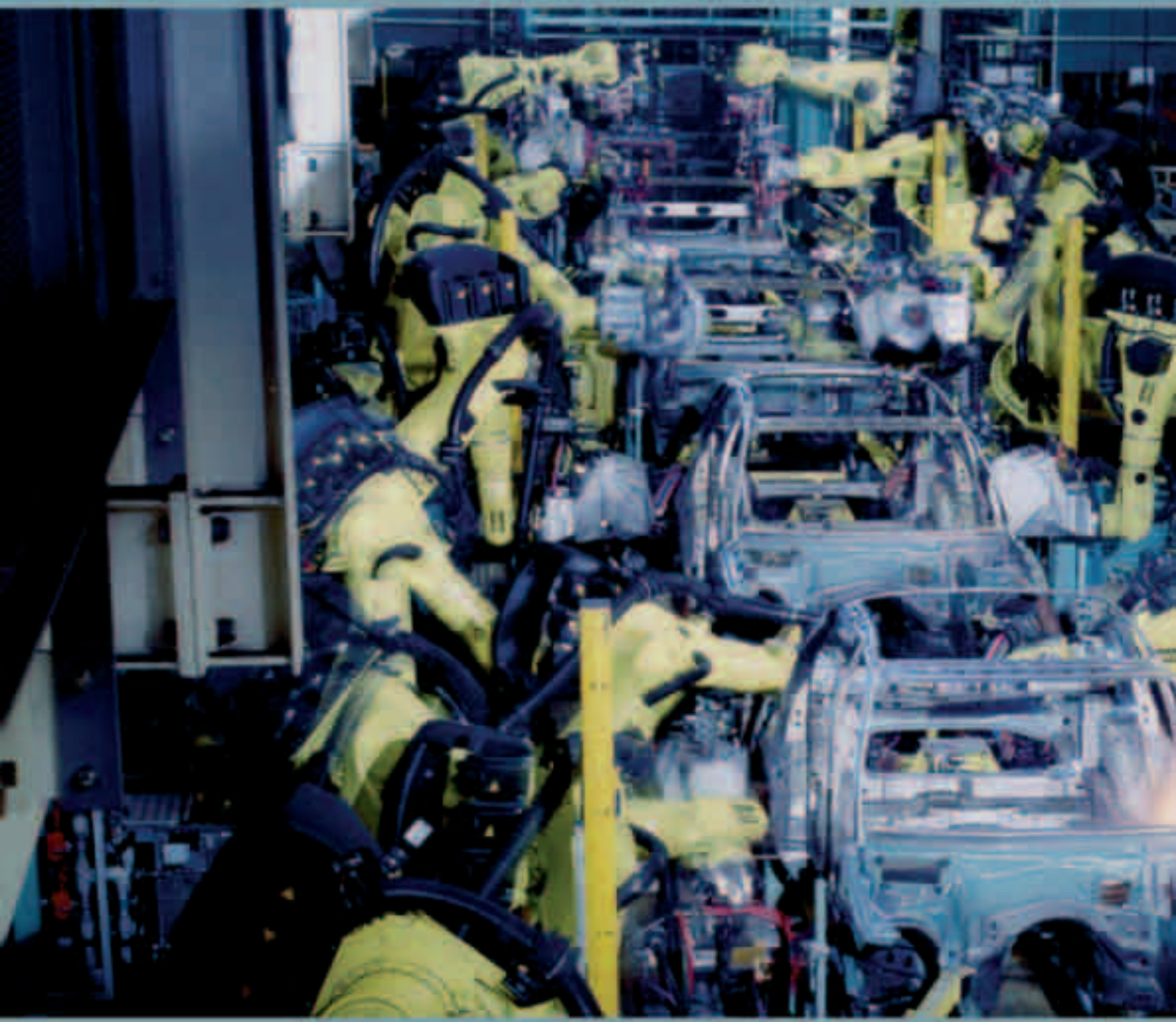
	ET 200S Motorstarter Standard	ET 200S High Feature / Failsafe
Stromeinstellung Ie	manuell, lokal am Schutzschalter	Weitbereich 0,3–3 A, 2,4–8 A, 2,4-16 A in 10 mA Schrittweite
Stromgrenzwertverletzungsverhalten	Abschalten	**Abschalten** mit/**ohne** Wiederanlauf Warnen
Abschaltklasse	CLASS 10	**CLASS** 10/20 (10A/10 bei DSS1e-x)
Pausenzeit	-	1-255 s/**deaktiviert** Möglichkeit das thermische Überlastmodell zu löschen
Nullstromerkennung	-	Verhalten Warnen/**Abschalten**
Unsymmetrie	Über Thermoauslöser	Warnen/**Abschalten**
Unterer, Oberer Stromgrenzwert	-	18,75% bis 100% Ie 50% bis 150% Ie
Motorstrommesswert	-	Übertragbar via Bus

Reaktionszeiten

Mit der hohen internen Datenübertragungsrate und dem 12 Mbaud Anschluss des ET 200S Interfacemodul an PROFIBUS DP wird der Einsatz der ET 200S Safety Motorstarter Solution in extrem zeitkritischen Applikationen ermöglicht.

Außerdem lassen sich die ET 200S Motorstarter mit Erweiterungsmodulen modular ausbauen. Zum Beispiel verkürzt das Bremsmodul mit oder ohne autark wirkende Schnellstop-Eingänge die Reaktionszeit von Antrieben, die besonders schnell schalten bzw. bremsen müssen. So lassen sich Montagebänder genauer positionieren oder eine Schiebersteuerung kann ganz einfach realisiert werden.

• Mindestbefehldauer PM-D F1, F2	200 ms
• Einschaltverzögerung PM-D F3 bis 5	< 150 ms
• Wiederbereitschaftszeit	
bei PM-D F1, F2	< 1 s
bei PM-D F3 bis 5	< 50 ms
• Rückfallverzögerung	
bei PM-D F1, F2, F4	30 ms
bei PM-D F3	0,5 bis 30 s (stufenlos einstellbar)
• Hilfsstromkreis U2 PM-D F1, F2, F4 und F5	
Bemessungsbetriebsstrom	4 A
Thermischer Dauerstrom	5 A
• PM-D F PROFIsafe	
Summenstrom der Ausgänge	5 A (Dauerstrom) / 10 A
Interne Datenverarbeitungsdauer	3 ms < T < 9 ms
Bemessungsbetriebsstrom eines SGs	2 A
• Motorstarter Failsafe Stromaufnahme aus SG1...6	
Anzug	250 mA (für 200 ms)
Halten	max. 55 mA
• Motorstarter Failsafe Stromaufnahme aus U1 (Elektronik Versorgung)	
Direktstarter	40 mA
Reversierstarter	100 mA



6.1 SIGUARD Laserscanner LS4
6.2 SIGUARD Lichtvorhänge und Lichtgitter
6.3 SIGUARD Lichtschranken
6.4 SIGUARD Schaltleisten

Fehlersichere optische Sensoren

6

sigurd

6 Fehlersichere optische Sensoren

6.1 SIGUARD Laserscanner LS4

Übersicht

Der SIGUARD Laserscanner ist ein berührungslos wirkendes Schutzsystem zur Absicherung von Gefahrenbereichen an stationären Maschinen und Anlagen sowie an mobilen Systemen.

Der Scanner ist ein optischer Distanzsensor und sendet innerhalb eines Arbeitsfeldes von 190° periodisch Lichtimpulse aus. Treffen die Impulse auf ein Hindernis oder eine Person, wird das Licht reflektiert und von dem Laserscanner empfangen und ausgewertet. Aus der Lichtlaufzeit berechnet der Scanner die genauen Koordinaten des „gesehenen" Hindernisses. Befindet sich das Hindernis bzw. die Person innerhalb definierter Bereiche, wird eine Stop-Funktion ausgeführt. Dabei werden die Halbleiterschaltausgänge innerhalb der Systemreaktionszeit abgeschaltet. Die Stop-Funktion wird, abhängig von der Betriebsart, bei freiem Schutzfeld selbsttätig oder nach Quittierung wieder zurückgesetzt.

Bild 6/1
SIGUARD Laserscanner LS4

Der SIGUARD Laserscanner kann Personen bis zu einer Entfernung von 4,0 m sicher erkennen, selbst dann, wenn sie sehr dunkle Kleidung tragen. Der Scanner ist durch den Einsatz dieses so genannten sicherheitsrelevanten Schutzfeldes für den Personenschutz konzipiert. Nicht sicherheitsrelevante Objekte können bis zu einer Entfernung von 15 m erkannt werden. Vier programmierbare Schutzfeldpaare ermöglichen es, den Schutzbereich optimal an die Applikationen anzupassen. Unter einem Feldpaar wird die Kombination aus einem Vorwarnfeld (Objektschutzfeld) und einem Schutzfeld (Personenschutzfeld) verstanden. Der Scanner kann sowohl an Fahrzeugen (fahrerlose Transportsysteme, Verschiebewagen) als auch stationär (Absicherung von Gefahrenbereichen an Maschinen) eingesetzt werden. Das berührungslose Messprinzip macht den SIGUARD Scanner damit zu einer universell einsetzbaren Schutzeinrichtung.

- Berührungslose, zuverlässige Sicherung von Gefahrenbereichen universell einsetzbar: an Maschinen, Fertigungsrobotern, Förderanlagen, Fahrzeugen etc.
- Standardvariante mit fehlersicheren Halbleiterausgängen
- Komfortable Variante mit PROFIBUS-Anschluss Profil PROFIsafe
- Automatische Parameterübertragung über PROFIBUS bei Gerätetausch
- Kategorie 3 nach EN 954-1
- Bis zu 4 Personenschutz- und Warnfeldpaare frei einstellbar
- Schutzfeld mit 4 Meter maximalem Radius für Personensicherheit
- Extrem kleine Bauform
- Geringe Stromaufnahme

Stationäre Gefahrenbereichsabsicherung

In modernen Produktionsanlagen ergibt sich häufig das Problem, dass gefährliche Bereiche von Personen betreten werden müssen. Während des Aufenthaltes in einem solchen Bereich muss sichergestellt sein, dass von der Maschine oder Anlage keine Personengefährdung ausgeht. Die dazu erforderlichen Sicherheitsvorkehrungen sollen jedoch den Produktionsablauf nicht behindern.

Der SIGUARD Laserscanner ermöglicht diese flexible, berührungslose Gefahrenbereichsabsicherung.

Bild 6/2
Stationäre Absicherung

Horizontale Gefahrenbereichssicherung

- Sicheres Erkennen von Personen und Objekten in Gefahrenbereichen von Maschinen und Anlagen
- Flexible Programmierung weitgehend beliebiger Schutz- und Warnfelder

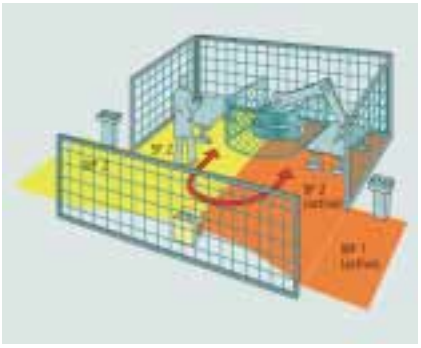


Bild 6/3
Horizontale Absicherung

Horizontale Gefahrenbereichssicherung mit mehreren Schutzfeldern

- Sicheres Erkennen von Personen in unterschiedlichen Gefahrenbereichen durch Umschalten der Schutzfelder
- Erhöhung der Verfügbarkeit durch gezielte Absicherung nur der gerade aktiven Bereiche

Mobile Absicherung fahrerloser Transportfahrzeuge

An fahrerlosen Transportfahrzeugen dient der SIGUARD Laserscanner LS4-4 zur Überwachung des Fahrweges. Dabei sollen Personen oder Objekte erkannt und das Fahrzeug selbsttätig zum Stillstand gebracht werden. Bisherige Schutzsysteme wie Bumper, Schutzbügel etc. erlauben nur eine geringe Fahrgeschwindigkeit. Mit dem SIGUARD Laserscanner LS4-4 als berührungsloser „voreilender Stoßfänger" jedoch, ergibt sich ein weitaus größerer Sicherheitsbereich. Die Fahrzeuge können schneller fahren, die Stillstandzeiten werden auf das notwendige Minimum reduziert.

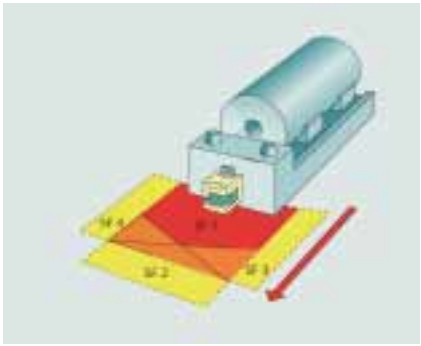


Bild 6/4

Fahrweg-Überwachung bei fahrerlosen Transportsystemen

- Sicheres Erkennen von Personen und Objekten, die sich dem Fahrzeug nähern
- Gegenüber Bumpern oder Schutzbügeln bietet der Laserscanner einen größeren Sicherheitsbereich und erlaubt daher eine höhere Geschwindigkeit

Bild 6/5

Kollisionsschutz bei Verschiebewagen

- Zuverlässiger Schutz von im Fahrweg befindlichen Personen
- Im Fahrweg befindliche Objekte werden rechtzeitig erkannt und Beschädigungen an Fahrzeug oder Ladung vermieden

Produktfamilien/Produktgruppen

SIGURARD Laserscanner LS4-4 Standardvariante

Fehlersichere Halbleiterausgänge
Inkl. Software LS4soft

3RG7834-6DD00

SIGURARD Laserscanner LS4-4 ASIsafe

Fehlersichere Direktanschluss an ASIsafe
Inkl. Software LS4soft

3SF7834-6DD00

SIGURARD Laserscanner LS4-4 PROFIsafe

Fehlersichere Direktanschluss an PROFIBUS
Inkl. Software LS4soft

3SF7834-6PB00

Bild 6/6

Der SIGUARD Laserscanner LS4 ist in drei verschiedenen Varianten erhältlich. Je nachdem wie der Scanner elektrisch in die Sicherheitsschaltung eingebunden werden soll, kann die entsprechende Variante ausgewählt werden. In ihrer Funktion als Laserscanner zur Gefahrenbereichssicherung unterscheiden sich die Geräte dabei nicht.

In der Standard-Variante verfügt der Scanner über zwei fehlersichere, selbstüberwachende Halbleiterausgänge, die eine Einbindung in konventioneller Schaltungstechnik ermöglichen.

Die Busversionen für AS-Interface erlaubt die fehlersichere Direktanbindung an ASIsafe.

Die sicherheitsgerichtete Abschaltung erfolgt hier über den AS-Interface Sicherheitsmonitor.

Die zweite busfähige Variante verbindet den Laserscanner mit PROFIBUS. Der fehlersichere Datenaustausch in beide Richtungen erfolgt mittels des herstellerneutralen Profils PROFIsafe. Sowohl das sicherheitsrelevante Abschaltsignal als auch die Schutzfeldumschaltung können, gesteuert von der fehlersicheren SPS, fehlersicher über den Bus übertragen werden.

Zu den SIGUARD Laserscannern gehört auch ein Programm von Zubehörteilen wie Montagehalterungen, Software sowie Anschluss- und Programmierkabel.

Einzelheiten zum Zubehör sowie weitere Unterlagen zu den SIGUARD Laserscannern finden Sie im Internet unter: http://www.siemens.de/fas

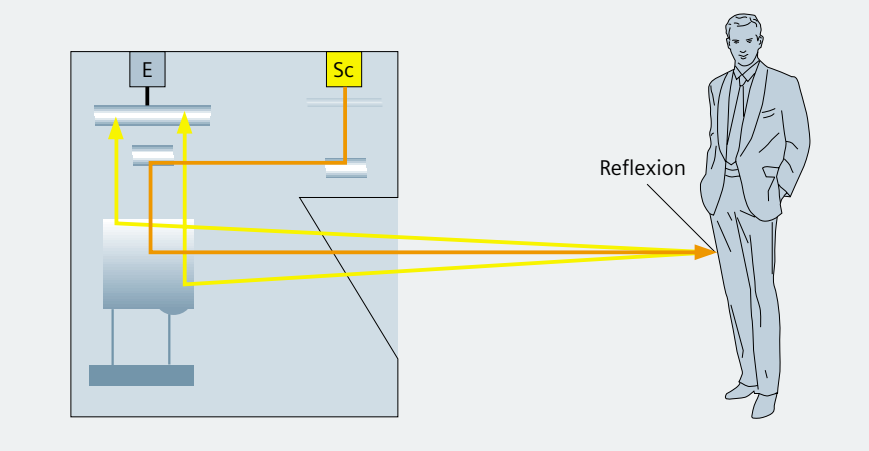


Bild 6/7
Funktionsprinzip

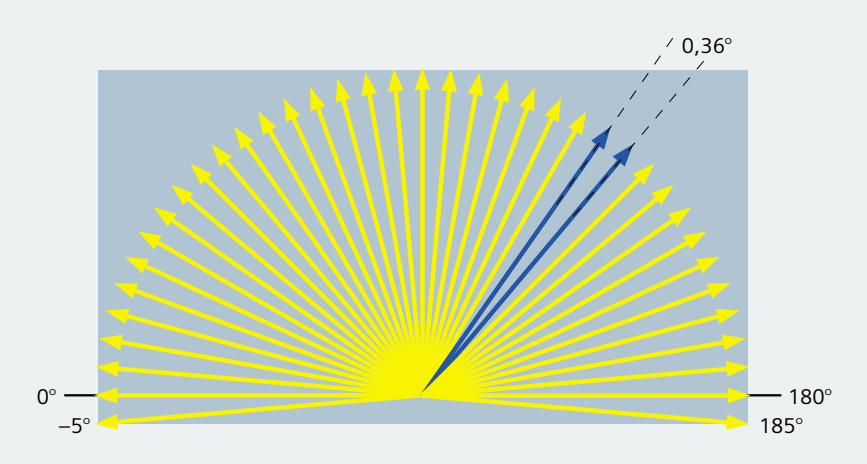


Bild 6/8
Winkelauflösung

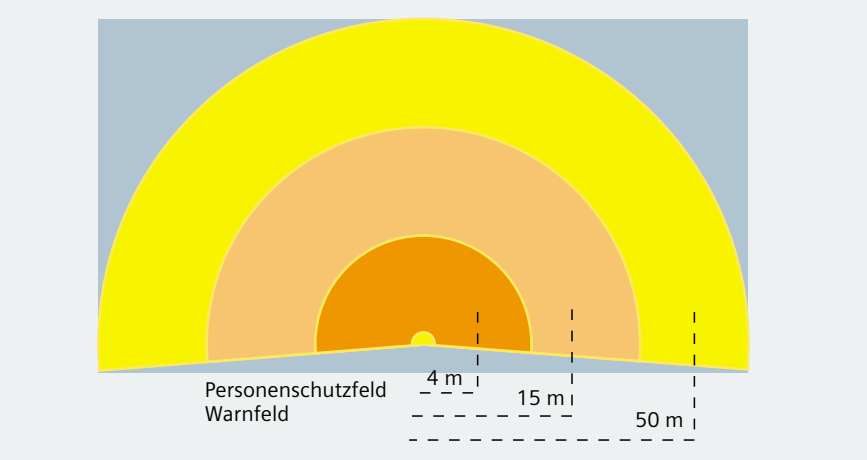


Bild 6/9
Schutz-Warnfelder

Aufbau

Der SIGUARD Laserscanner LS4 ist ein optischer, berührungslos arbeitender Flächenscanner – in erster Linie konzipiert für den Personenschutz. Über eine Laserdiode mit Sendeoptik erzeugt der Laserscanner fortlaufend gebündelte Lichtimpulse, die ein integrierter Drehspiegel in den gesamten Arbeitsbereich streut. Dringen Objekte oder Personen in das Feld ein, wertet er die reflektierten Lichtimpulse aus und berechnet anhand der Lichtlaufzeit laufend die exakten Positionskoordinaten. Wird das definierte Personenschutzfeld verletzt, veranlasst er ein Abschaltsignalfür einen sofortigen Maschinenstop.

Der Arbeitsbereich des SIGUARD Laserscanners LS4 erstreckt sich über 190° und ist in Winkelsegmente von 0,36° aufgeteilt. Die Scanrate beträgt 25 Scans pro Sekunde, das heißt alle 40 ms ein Lichtimpuls in jedem Segment. Ein spezieller Algorithmus stellt dabei sicher, dass Objekte ab einer Größe von 70 mm – das entspricht der Auflösung des Scanners – sicher erkannt werden, dabei aber Störeinflüsse wie Staub o. ä. die Verfügbarkeit der Anlage nicht herabsetzen.

Der SIGUARD Laserscanner LS4 erkennt zuverlässig Personen – selbst bei dunkler Bekleidung – sicherheitsgerichtet bis auf 4 Meter Entfernung. Bis zu einer Distanz von 15 Meter können Personen und Objekte darüber hinaus, zum Beispiel zur Ausgabe einer Warnmeldung, erfasst werden (nicht sicherheitsgerichtet).

Funktionen

Schutzfeldumschaltung

Durch vier variable – einfach am PC erstellbare – Schutzfeldpaare für Personenschutzfeld und Warnfeld ist der SIGUARD Laserscanner an jede Anforderung flexibel anpassbar. Er ist stationär an Maschinen und Anlagen einsetzbar, aber auch mobil an Fahrzeugen, fahrerlosen Transportsystemen oder Verschiebewagen. So können beispielsweise bei einem Roboter verschiedene Arbeitsbereiche abgesichert werden, in denen der Laserscanner zeitlich und räumlich nacheinander arbeitet. Bei fahrerlosen Transportsystemen lassen sich mit vier programmierten Schutzfeldern z.B. schnelle Fahrt, langsame Fahrt, Linkskurven und Rechtskurven absichern.

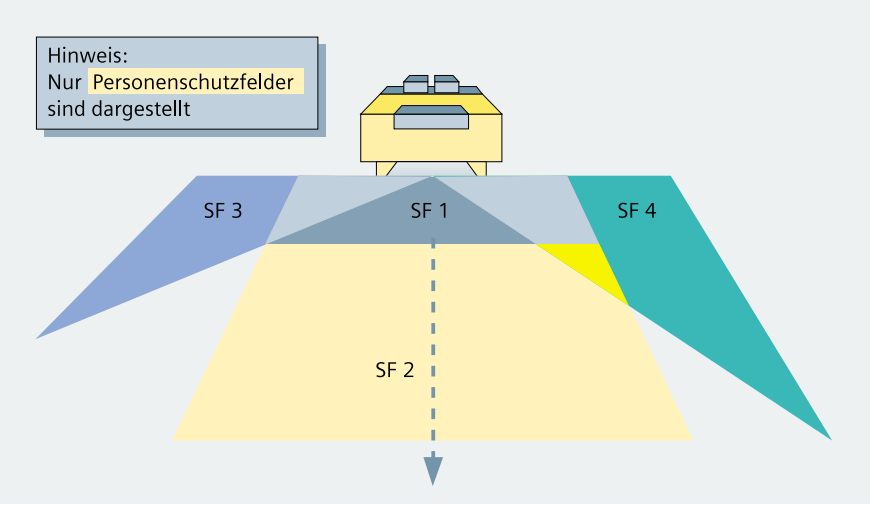


Bild 6/10
Schutzfelder

Wiederanlaufsperre

Der Laserscanner LS4 bietet die Funktion der Wiederanlaufsperre. Diese an- oder abwählbare Funktion ist vorgesehen, um den Wiederanlauf der Maschine an eine manuelle Zustimmung zu koppeln. Die Wirksamkeit betrifft alle Schutzfelder und ist unabhängig von etwaigen Schutzfeldumschaltungen.

Der entsprechende Taster ist so anzubringen, dass

- von der Bedienposition aus der gesamte Gefahrbereich bzw. die Schutzfeldschwäche eingesehen werden kann,
- von der Bedienposition kein direkter Zutritt/Zugriff zum Gefahrbereich bzw. zur Gefahrenstelle möglich ist.

Restart

Der Restart-Eingang hat je nach Betriebszustand mehrere Funktionen:

- Freigabe der Wiederanlaufsperre nach einer Schutzfeldverletzung
- Freigabe der Anlaufsperre nach einem Systemstart
- Neustart nach dem Beheben einer Gerätestörung
- Erkennen eines definierten Freigabesignals
  - nach einer Gerätestörung
  - nach einer Schutzfeldverletzung

  zum Lösen der Wiederanlaufsperre

Komfortable Parametriersoftware LS4soft

Die Bedien- und Parametriersoftware LS4soft erlaubt die Einstellung der Parameterdaten und der Schutz- und Warnfelder des Laserscanners.

- Komfortable Schutzfeldkonfiguration mittels PC oder Laptop
- Konfiguration weiterer Funktionen wie Schutzfeldumschaltung, Wiederanlaufsperre etc. mit Hilfe eines Software-Assistenten
- Umfassende Anzeigen – z.B. definierte Schutzfelder, aktuelle Scan-Kontur, Systemeinstellungen etc.
- Sicherer Zugriffsschutz durch Passwörter mit unterschiedlichen Berechtigungsstufen
- Lauffähig unter Microsoft Windows 95/98/2000/NT/XP

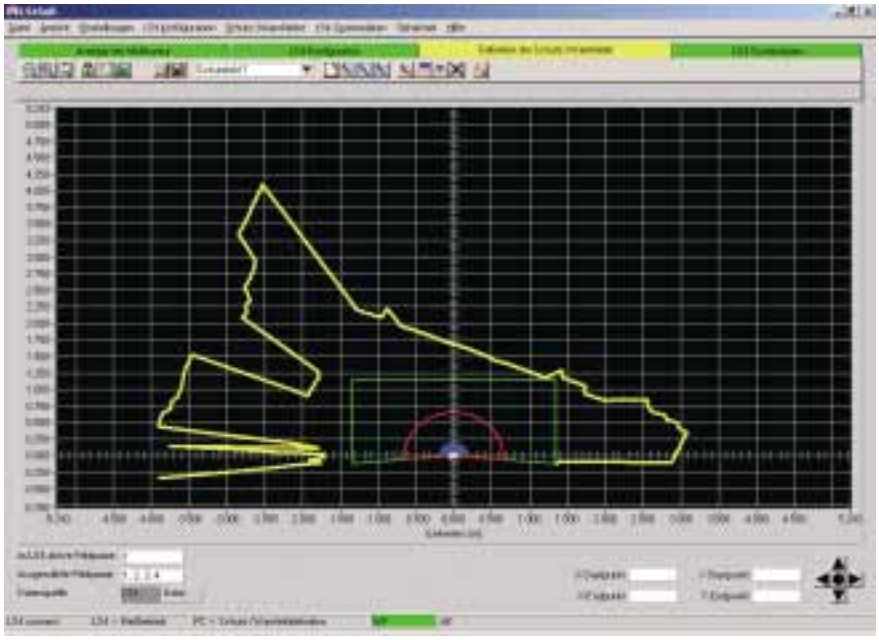


Bild 6/11
Software LS4Soft

Systemeinbindung

Je nach Anforderung und Art der vom Anwender gewählten Sicherheitstechnik lässt sich Sicherheitssensoren auf verschiedene Weisen elektrisch in die Sicherheitsschaltung der jeweiligen Maschine oder Anlage einbinden.

In Kapitel 3 werden die verschiedenen grundsätzlichen Arten der Sensoreinbindung beschrieben. Der SIGUARD Laserscanner bietet hier alle Möglichkeiten. Neben der kostengünstigen, konventionellen Anschaltung über fehlersichere Halbleiterausgänge erlauben die busfähigen Varianten die durchgängige, fehlersichere Einbindung in die Siemens Automatisierungslösungen über die Standard-Bussysteme AS-Interface und PROFIBUS.

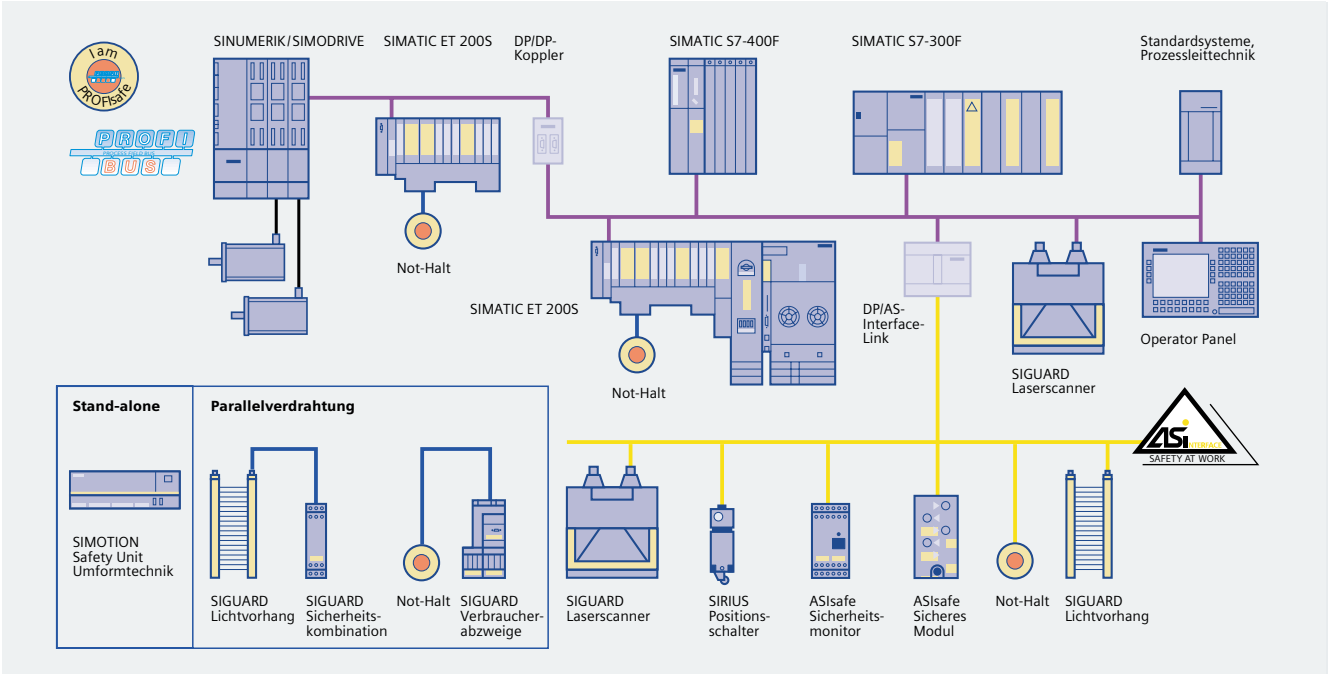


Bild 6/12
Systemeinbindung

Anwendungshinweise

Der SIGUARD Laserscanner ist ein berührungslos wirkendes Schutzsystem, bei deren Anwendung die Bedingungen zu einem bestimmungsgemäßen Gebrauch beachtet werden müssen.

Im Folgenden sind einige der wesentlichen Punkte aufgeführt:

Allgemeine Hinweise:

- Der SIGUARD Laserscanner LS4-4 ist so anzubringen, dass der Zutritt zum zu überwachenden Gefahrenbereich durch das Schutzfeld komplett abgedeckt wird.
- Die Montageposition des Scanners muss vor Feuchte, Verschmutzungen, sowie Temperaturen unter 0°C bzw. über 50°C Schutz bieten.
- Der Montageort ist so zu wählen, dass die Möglichkeiten mechanischer Beschädigungen minimiert werden. An exponierten Stellen sind zusätzliche Schutzverkleidungen oder -bügel vorzusehen.
- Bewehrungen, Verkleidungen, Montagenischen und andere Maschinenelemente dürfen nicht zu einer Beeinträchtigung des Scanner-Blickfeldes führen.
- Befinden sich Abschattungsflächen wegen feststehender Hindernisse, die als Schutzfeldbegrenzung definiert wurden, sollten diese so gesichert werden (z.B. durch Schutzgitter), dass darin stehende Personen nicht plötzlich in das Schutzfeld treten können. In der Gefährdungsanalyse zur Maschine oder Anlage muss dieser Punkt beachtet werden.
- Retro-Reflektoren oder stark glänzende Oberflächen wie bestimmte Metalle oder Keramiken in Schutzfeldnähe und in Höhe der Scanebene sind zu vermeiden, da durch sie Messfehler entstehen können.
- Um eine gleichbleibende Detektionshöhe an jedem Punkt des Schutzfeldes sicherzustellen, ist der Scanner – und damit die Strahlebene – parallel zur Bezugsebene zu montieren.
- Ist die Funktion „Wiederanlaufsperre" vorgesehen, muss der Wiederanlauftaster außerhalb des Schutzfeldes an einer Stelle angebracht werden, von der aus der gesamte Gefahrenbereich einsehbar ist.

Hinweise zur Schutzfeldumschaltung:

Im Zuge einer optimalen Maschinenauslastung erfolgt oft ein wechselweiser Beschickungs-/Bearbeitungszyklus, welcher sich verändernde Gefahrenbereiche mit sich bringt. Auch FTF-Anwendungen (Führerlose Transport Fahrzeuge) beinhalten naturgemäß verschiedene Gefahrenzonen. Ist nun mit einem Zutritt von Personen in diese Bereiche zu rechnen, besteht die Notwendigkeit eines sich anpassenden Sicherungssystems. Mit seinen je vier umschaltbaren und frei konfigurierbaren Schutz- und Warnfeldern (Feldpaaren) erfüllt der SIGUARD Laserscanner LS4 vielfältige Anforderungen hinsichtlich der Absicherung unterschiedlichster Applikationen.

Die Festlegung der notwendigen Feldpaarkonturen ist durch das komfortable Bedienerprogramm „LS4soft" möglich.

Aktiviert werden die Feldpaare über das Anlegen von 24 V auf die entsprechenden Eingänge.

Soll der SIGUARD Laserscanner LS4-4 neu gestartet oder zwischen verschiedenen Feldpaaren umgeschaltet werden, sind folgende Punkte zu beachten:

- Das für den Start vorgesehene Feldpaar ist unter besonderer Beachtung der für diesen Moment gültigen Gefahrenbereiche festzulegen.
- Es ist immer zuerst das zweite Feldpaar dazu-, danach das erste Feldpaar abzuschalten.
- Die Umschaltung muss innerhalb von 1 s erfolgen.
- Der Schaltvorgang darf zu keiner Zeit die Deaktivierung aller Feldpaare beinhalten.
- Bis auf den Umschaltvorgang darf jeweils nur ein Feldpaar aktiv sein.
- Die Reihenfolge der zu aktivierenden Überwachungsfelder muss sicherstellen, dass zu keiner Zeit die applikationsbezogene Schutzfeldmindestgröße unterschritten wird.
- Umschaltsignale dürfen nicht durch einen systematischen Fehler gleichzeitig wechseln können. Dies wird erreicht durch den Einsatz unabhängiger Schaltkreise (z.B. getrennt betätigte binäre Schalter) unter Berücksichtigung des oben beschriebenen Schaltverhaltens.

Schutzfeldberechnung

Bei Einsatz von berührungslos wirkenden Schutzsystemen wie dem Laserscanner muss allgemein sichergestellt werden, dass eine gefahrbringende Maschinenbewegung angehalten wird, bevor eine Verletzung des Menschen erfolgen kann. Deswegen muss zum Beispiel durch den Laserscanner ein Schutzfeld überwacht werden, dass groß genug ist, um nach Betreten einen rechzeitigen Maschinenstop auslösen zu können.

Stationäre Gefahrenbereichsabsicherung

Für den Einsatz eines Laserscanners zur stationären Absicherung von Gefahrenbereichen müssen folgende Berechnungen zugrunde gelegt werden.

Bild 6/13
Stationäre Gefahrenbereichsabsicherung

Zur Berechnung des Sicherheitsabstandes und der Mindestschutzfeldtiefe gelten gemäß IEC 61496-3 und DIN EN 999 bei Annäherungsrichtung parallel zum Schutzfeld folgende Beziehungen:

Sicherheitsabstand

$S = (K \times T) + C$

$C = 1200\ mm - 0{,}4\ H$

$C_{MIN} = 850\ mm$
$H_{MIN} = 15\ (d - 50\ mm)$
$H_{MAX} = 1000\ mm$

S = Sicherheitsabstand, Mindestabstand vom Gefahrbereich zum Erkennungspunkt, zur Erkennungsebene oder zum Schutzfeld in mm

K = Annäherungsgeschwindigkeit einer Person bzw. deren Körperteilen in mm/s (1600 mm/s)

T = Nachlaufzeit des gesamten Systems (Ansprech- und Bremszeiten bis zum Stillstand) in s

C = Sicherheitsbezogene Konstante zur Berücksichtigung des Eindringens in den Gefahrbereich vor Auslösen der Schutzeinrichtung in mm

C_{MIN} = Minimalwert der sicherheitsbezogenen Konstante in mm (850 mm)

H = Höhe der Messwerterfassungsebene ab Bezugspunkt in mm

H_{MIN} = Mindesthöhe der Messwerterfassungsebene ab Bezugsebene in mm

H_{MAX} = Maximalhöhe der Messwerterfassungsebene ab Bezugsebene in mm

d = Auflösung des Scanners in mm (70 mm, schutzfeldweit)

Zuschläge

Die Summe der systemspezifischen und applikationsbedingten Schutzfeldzuschläge errechnet sich aus nachstehender Formel:

$Z_{GES} = Z_{SM} + Z_{REFL}$

Z_{GES} = Summe der systemspezifischen und applikationsbedingten Schutzfeldzuschläge in mm

Z_{SM} = Messfehler des Scanners in mm

Z_{REFL} = Zuschlag bei zu berücksichtigenden Reflektoren in mm

Schutzfeldtiefe

Die Schutzfeldtiefe, das heißt die Größe, die letztendlich für das im Scanner zu programmierende Schutzfeld relevant ist, errechnet sich aus nachstehender Formel:

$S_T = (K \times (T_{SCAN} + T_{MASCH} + (T_{NACHLAUF} \times L_{NACHLAUF}))) + C + Z_{GES}$

S_T = Schutzfeldtiefe, Abstand vom Gefahrbereich zum/zur Erkennungspunkt, -linie, inklusive der system- und applikationsbezogenen Zuschläge in mm

K = Annäherungsgeschwindigkeit einer Person bzw. derer Körperteile in mm/s (1600 mm/s)

T_{SCAN} = Reaktionszeit des Scanners in s

T_{MASCH} = Reaktionszeit der Maschine oder Anlage in s

$T_{NACHLAUF}$ = Nachlaufzeit des gesamten Systems in s

$L_{NACHLAUF}$ = Faktor für die Nachlauferhöhung (1,1 wenn keine anderen Werte bekannt sind)

C = sicherheitsbezogene Konstante in mm

Montagehöhe

Nach DIN EN 999 berechnet sich die niedrigste zulässige Höhe der Scanebene ab Standflächenebene für Personen nach folgender Formel:

$H_{MIN} = 15 * (d - 50\ mm)$

H_{MIN} = niedrigste zulässige Scanebene ab der Standflächenebene

d = Auflösung des Scanners in mm (70 mm, schutzfeldweit)

Der zulässige Höhenbereich der Scanebene liegt zwischen 300 und 1000 mm über der Standflächenebene.

Bedingt die Applikation eine höhere Scanebene als 300 mm oder besteht die Möglichkeit des Zutritts von Kindern, muss in der Gefahrbereichsanalyse eine Gefährdung durch Unterkriechen der Scanebene berücksichtigt werden.

Mobile Absicherung fahrerloser Transportfahrzeuge

Beim Einsatz des SIGUARD Laserscanners zur mobilen Absicherung zum Beispiel an fahrerlosen Transportsystemen müssen folgende wesentliche Bedingungen beachtet werden.

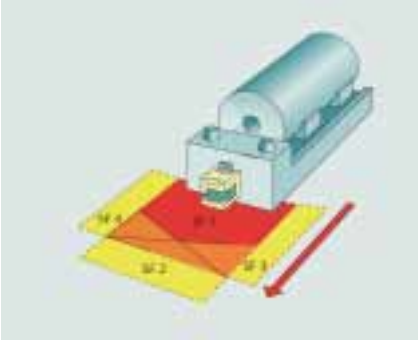


Bild 6/14

Sicherheitsabstand

Zur Berechnung des Sicherheitsabstandes gelten gemäß IEC 61496-3 folgende Beziehungen:

$S = (V_{MAXFTS} \times T) + S_{ANHALT}$

V_{MAXFTS} = maximale Geschwindigkeit des FTS in mm/s

T = Reaktionszeit des Scanners und des FTS in s

S_{ANHALT} = Anhalteweg des FTS bis zum Stillstand in mm

Schutzfeldtiefe

Die Tiefe des Schutzfeldes in Fahrtrichtung, bezogen auf die Entfernung zwischen der Fahrzeugbegrenzung und der Schutzfeldbegrenzungslinie, errechnet sich aus nachstehender Formel:

$S_T = V_{MAXFTS} \times (T_{SCAN} + T_{FTS}) + (S_{ANHALT} \times L_{ANHALT}) + Z_{GES}$

S_T = Schutzfeldtiefe in Fahrtrichtung in mm

V_{MAXFTS} = maximale Geschwindigkeit des FTS in mm/s

T_{SCAN} = Reaktionszeit des Scanners in s

T_{FTS} = Reaktionszeit des FTS in s

L_{ANHALT} = Faktor für den Bremsenverschleiß (1,1 wenn keine anderen Werte bekannt sind)

Z_{GES} = Summe der systemspezifischen und applikationsbedingten Zuschläge in mm

Zuschläge

$Z_{GES} = Z_{SM} + Z_{REFL} + Z_{AFUSS} + Z_{AU}$

Z_{SM} = Messfehler des Scanners in mm

Z_{REFL} = Zuschlag bei zu berücksichtigenden Reflektoren in mm

Z_{AFUSS} = Zuschlag für mangelnde Bodenfreiheit des FTS in mm

Z_{AU} = applikationsbedingter Zuschlag in mm (z.B. Unterschnitte)

Montagehöhe

Grundsätzlich sollte die Montagehöhe so niedrig wie möglich gewählt werden, um ein Unterkriechen des Schutzfeldes zu vermeiden. Diese Vorgabe wird eingeschränkt durch z.B. Bodenunebenheiten und Federwege des FTS.

Die maximale Montagehöhe ist so zu wählen, dass ein Objekt (liegender Zylinder mit einem Durchmesser von 200 mm) sicher detektiert wird (siehe DIN EN 1525). Dies ist bei der maximalen Schutzfeldtiefe zu kontrollieren. Hinsichtlich der ausreichenden Detektionsauflösung ist bei FTS-Applikationen ein Objekt (stehender Zylinder) mit einem Durchmesser von 70 mm, schutzfeldweit, ausreichend.

Die hier beschriebenen Beispiele geben das Grundprinzip der Schutzfeldberechnungen wieder. Detailliertere Informationen sowie Berechnungsbeispiele finden Sie in der Technischen Anleitung des SIGUARD Laserscannern im Internet unter:
http://www.siemens.de/fas

Technische Daten

Schutzdaten	
Personenschutzfeld	
Erkennungsbereich	0-4 m (keine Totzonen bei bestimmungsgemäßer Montage)
Remissionsvermögen	mind. 1,8 % (matt-schwarz)
Messfehler	max. 83 mm (bei Schutzradius < 3,5 m) max. 100 mm (bei Schutzradius > 3,5 m)
Objektgröße	70 mm (zylindrischer Probekörper)
Ansprechzeit	mind. 80 ms (bei Standardvariante)
Anzahl der Schutzfelder	4 (über Schalteingänge umschaltbar)
Ausgang	Zwei fehlersichere PNP-Transistorausgänge 24 V/250 mA bzw. sichere Busanbindung
Kategorie	Kategorie 3 nach EN 954-1, Typ 3 nach DIN EN IEC 61496-1, IEC 61496-3 Anforderungsklasse 4 nach DIN V 19250, einfehlersicher
Anlauf	Die Anlauftestung und die Anlaufsperre sind separat parametrierbar
Warnfeld	
Erkennungsbereich	0-15 m
Remissionsvermögen	mind. 20 %
Objektgröße	150 x 150 mm
Ansprechzeit	mind. 80 ms (entspricht 2 Scans)
Anzahl der Schutzfelder	4 (über Schalteingänge umschaltbar)
Ausgang	PNP-Transistorausgang, max. 100mA bzw. Busanbindung
Optische Eigenschaften	
Winkelbereich	190°
Winkelauflösung	0,36°
Scanrate	25 Scans/s bzw. 40 ms/Scan
Laserschutzklasse	Klasse 1 (augensicher), DIN EN 60825-1, Wellenlänge = 905nm, Strahldivergenz = 2mrad, Zeitbasis = 100 s

Allgemeine Daten

	Standard	AS-Interface	PROFIBUS
Elektrische Versorgung			
Spannungsversorgung	+24 V DC +20 % / -30 %, Versorgung nach IEC 742 mit Sicherheitstrafo oder		
	vergleichbar bei DC/DC-Konvertern		
Überstromschutz	über Sicherung 1,25 A mittelträge im Schaltschrank		
Stromaufnahme	ca. 300 mA	ca. 350 mA	ca. 350 mA
(Netzteil mit 2,5 A verwenden)			
Leistungsaufnahme	ca. 8 W bei 24 V	ca. 9 W bei 24 V	ca. 9 W bei 24 V
	zuzüglich der Ausgangsbelastung		
Eingänge			
Restart/Reset	Anschluss eines Befehlsgerätes für Betriebsart “mit Wiederanlaufsperre” und/oder Geräteset, dynamisch überwacht		
Feldpaarumschaltung	Auswahl von 4 Feldpaaren über 4 Steuerleitungen mit interner Überwachung (Feldpaar = 1 Schutzfeld und 1 Warnfeld), 24 V DC optoentkoppelt	Auswahl von 4 Feldpaaren über 4 Steuerleitungen mit interner Überwachung (Feldpaar = 1 Schutzfeld und 1 Warnfeld), 24 V DC optoentkoppelt	Feldpaarumschaltung über PROFIBUS (Profil PROFIsafe)
Ausgänge			
Schutzfeld	2 x sicherer Halbleiterausgang, PNP max. 250 mA kurzschlussüberwacht, überstromgeschützt	AS-Interface, sicherer Slave (ASIsafe)	PROFIBUS, sicherer Slave (Profil PROFIsafe)
Warnfeld/ Verschmutzung/Störung	PNP-Transistorausgang max. 100 mA	AS-Interface	PROFIBUS
Software			
Bediener-Software	Kommunikations- und Parametrier-Software LS4soft unter Windows 95/98/2000/NT/XP		
	mit sicherem Protokoll zur Programmierung		
Schnittstellen			
RS 232, RS 422	Zur Geräteparametrierung und Felddefinition mittels LS4soft (RS 422 nur bei Standardvarianten)		
Umgebung und Material			
Schutzart	IP 65 nach IEC 60529		
Berührungsschutz	Schutzklasse 2		
Betriebstemperatur	0 ... + 50°C		
Lagertemperatur	- 20°C ... + 60°C		
Feuchte	DIN 40040 Tabelle 10, Kennbuchstabe E (mäßig trocken)		
Abmessung (B x H x T) in mm	140 x 155 x 135	140 x 168 x 165	140 x 168 x 165

6.2 SIGUARD Lichtvorhänge und Lichtgitter

Relevante Normen

- EN 61 496-1, -2, IEC 61 496-1, -2 (Anforderungen für berührungslos wirkende Schutzsysteme)
- EN 999 (u.a. Berechnung der Sicherheitsabstände)
- EN 954-1 (Sicherheit von Maschinen, sicherheitsbezogene Teile von Steuerungen)

Bild 6/15
SIGUARD Lichtvorhänge, Lichtgitter und Auswertegeräte

SIGUARD Lichtvorhänge und Lichtgitter

- sind aktive optoelektronische Schutzeinrichtungen (AOPD)
- entsprechen Typ 2 (3RG78 41) bzw. Typ 4 (3RG78 42/4) nach EN 61496-1, -2
- sind EG-baumustergeprüft
- schützen das Bedienpersonal an oder in der Nähe von gefährlichen Maschinen
- wirken berührungslos
- sind verschleißfrei im Vergleich zu mech. Systemen (z.B. Trittmatten)

Voraussetzungen hierfür sind:

- Die richtige Montage
- Die korrekte Einbindung in die Maschinensteuerung

Hinweise hierzu finden Sie in diesem Kapitel und in den Betriebsanleitungen zu den jeweiligen Geräten.

Prüfungen/Service

Die Geräte sind EG-Baumustergeprüft (TÜV Product Service in Zusammenarbeit mit dem Berufsgenossenschaftlichen Institut für Arbeitssicherheit BIA)

Konfiguration

- Durch Teach-in über optomagnetischen Schlüssel
- Übertragung der Konfigurierdaten durch eine steckbare Konfigurationskarte

Merkmale

SIGUARD Lichtvorhänge, -gitter und Transceiver 3RG7844/ 3SF7844 mit integrierter Auswertung für Kategorie 4 nach EN 954-1

- Auflösung 14, 30 und 50 mm
  Schutzfeldhöhen von 150 bis 3 000 mm
  Reichweiten 0,3 bis 6 m bzw. 0,8 bis 18 m
- 2-, 3- oder 4-strahlige Lichtgitter
  Strahlabstand 500, 400 und 300 mm
  Reichweiten 0,8 bis 18 m bzw. 6 bis 70 m
- 2-strahliger Transceiver
  Strahlabstand 500 mm
  Reichweite 0,8 bis 6 m
- Kaskadierung von Host- und Guestgeräten für größere Schutzfeldhöhen bzw. –längen oder für eine winklige Anordnung

Integrierte Funktionen:

Funktionspaket Standard
- Anlauf-/Wiederanlaufsperre
- Schützkontrolle
- Multi-Scan

Funktionspaket Blanking
- Funktionen des Funktionspaketes Standard und zusätzlich
- Fixed Blanking
- Floating Blanking
- Reduced Resolution

Funktionspaket Muting
- Funktionen des Funktionspaketes Standard und zusätzlich
- 4-Sensor Sequenziell Muting
- 2-Sensor Parallel Muting
- 3-Sensor-Richtungs-Muting
- 4-Sensor-Parallel-Muting

Funktionspaket Taktsteuerung
- Funktionen des Funktionspaketes Standard und zusätzlich
- Taktsteuerung durch 1-Takt- und 2-Taktbetrieb

Konfiguration:

- Durch Teach-in über einen optomagnetischen Schlüssel
- Übertragung der Konfigurierdaten durch eine steckbare Konfigurationskarte
- 2 Übertragungskanäle
- Kaskadierung von Host- und Guest-Geräten
- Erweitertes Display (2x7-Segmente)

Für jedes Funktionspaket verfügbare Ausgänge/Anschlüsse

- Local-Interface zum Anschluss weiterer Sicherheits-Sensoren
- Transistorausgänge mit Kabelverschraubung bzw. Brad-Harrison-Stecker
- Relaisausgänge mit Hirschmann-Stecker
- Anschluss an ASIsafe

SIGUARD Lichtvorhänge, -gitter 3RG7842/3SF7842 für Kategorie 4 nach EN 954-1

- Auflösung 14, 30, 50 und 90 mm Schutzfeldhöhen von 150 bis 3 000 mm Reichweiten 0,3 bis 6 m bzw. 0,8 bis 18 m

- 2-, 3- oder 4-strahlige Lichtgitter Strahlabstand 500, 400 und 300 mm Reichweiten 0,8 bis 18 m bzw. 6 bis 70 m

- Kaskadierung von Host- und Guest-geräten für größere Schutzfeldhöhen bzw. –längen oder für eine winklige Anordnung

SIGUARD Lichtvorhänge 3RG7841 für Kategorie 2 nach EN 954-1

- Auflösung 30, 55 und 80 mm Schutzfeldhöhen von 150 bis 1 800 mm Reichweiten 0,3 bis 6 m

- Kaskadierung von Host- und Guest-geräten für größere Schutzfeldhöhen bzw. -längen oder für eine winklige Anordnung

SIGUARD Auswertegeräte 3RG7825/47 für Kategorie 2 und 4 nach EN 954-1

- Dienen zur Einbindung der sicheren Signale der Lichtvorhänge, Lichtgitter, Lichtschranken und Transceiver in die Maschinensteuerung.

- Anlauf-/Wiederanlaufsperre

- Schützkontrolle

- Muting

- Taktsteuerung

- Vorausfallwarnung für die Relaiskontakte

- Diagnosefunktion mittels PC

- Zahlreiche Meldeausgänge zu einer übergeordneten Steuerung

Anwendungsbereich

Lichtvorhänge für Finger- und Handschutz an Gefahrenstellen

Schutz vor Eingreifen in Gefahrenstellen bei Montage der Lichtvorhänge nahe am gefahrbringenden Maschinenteil (Finger- und Handschutz)

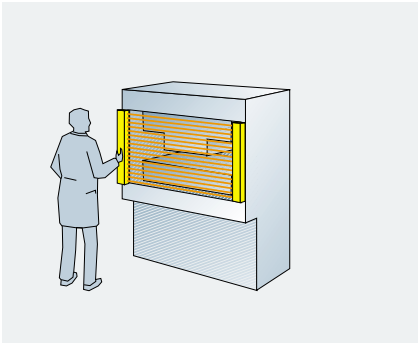


Bild 6/16
Finger-Handschutz

Geräteauswahl

Lichtvorhänge für Kategorie 2 oder 4 mit 14 und 30 mm Auflösung

Anwendungsbereiche

z.B. Pressen, Stanzen, Filterpressen, Schneidemaschinen

Lichtvorhänge zur horizontalen Gefahrenbereichssicherung

Sicheres Erkennen von Personen in Gefahrenbereichen bei Montage des Lichtvorhangs in Bodennähe (kein Unterkriechen möglich)

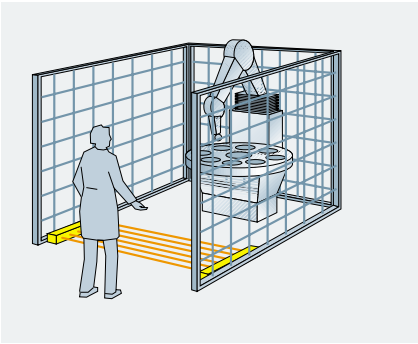


Bild 6/17
Gefahrenbereichsschutz 50 mm

Geräteauswahl

Lichtvorhänge für Kategorie 2 oder 4 mit 50 bzw. 55 mm Auflösung

Anwendungsbereiche

z.B. Schweiß- und Montagelinien sowie -roboter im Automobilbau

Lichtvorhänge zur horizontalen Gefahrenbereichssicherung

Sicheres Erkennen von Personen in Gefahrenbereichen bei Montage des Lichtvorhangs in Höhen von 0,6 bis 1 m

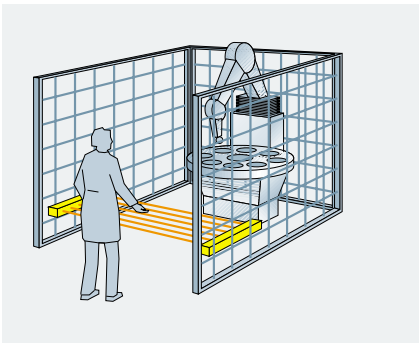


Bild 6/18
Gefahrenbereichsschutz 90 mm

Geräteauswahl

Lichtvorhänge für Kategorie 2 oder 4 mit 80 bzw. 90 mm Auflösung

Anwendungsbereiche

z.B. Schweiß- und Montagelinien sowie -roboter im Automobilbau

Lichtgitter zur Zugangssicherung

Sicheres Erkennen von Personen bei Zutritt zu Gefahrenbereichen

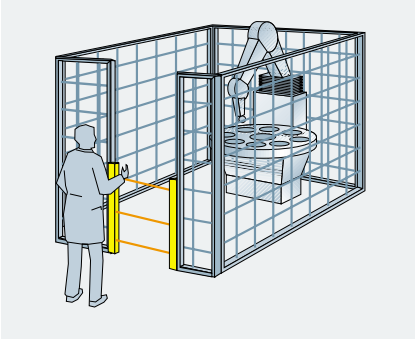


Bild 6/19
Zugangsschutz 18 m

Geräteauswahl

2-, 3- oder 4-strahlige Lichtgitter für Kategorie 4 mit 18 m Reichweite

Anwendungsbereiche

Zugangssicherung, z.B. an Robotern oder Handlingsautomaten

Lichtgitter zur Zugangssicherung für große Bereiche

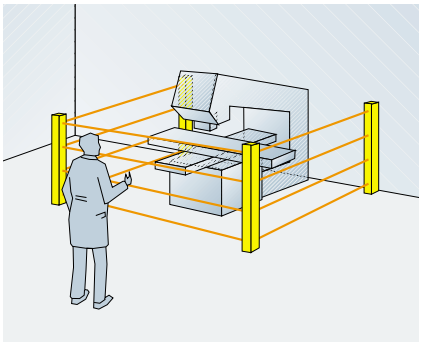


Bild 6/20
Zugangsschutz 60 m

Sicheres Erkennen von Personen bei Zutritt zu Gefahrenbereichen.

Absicherung größerer Gefahrenbereiche durch hohe Reichweite von 70 m.

Geräteauswahl

2-, 3- oder 4-strahlige Lichtgitter für Kategorie 4 mit bis zu 70 m Reichweite.

Anwendungsbereiche

Zugangssicherung, z.B. an automatischen Bearbeitungszentren oder Palletieranlagen.

Folgende Faktoren müssen für den Einsatz von Lichtsystemen gegeben sein:

- Ein Übergreifen, Untergreifen und Hintertreten des Schutzfeldes muss ausgeschlossen sein, eventuell sind zusätzliche Schutzeinrichtungen anzubringen.
- Die Steuerung der Maschine muss elektrisch beeinflussbar sein und in jeder Arbeitsphase ein sofortiges Beenden des gefahrbringenden Zustandes zulassen.
- Verletzungsgefahr durch Wärme, Strahlung bzw. Ausstoß von Materialien und Bestandteilen aus der Maschine muss anderweitig ausgeschlossen werden.
- Umgebungsbedingungen dürfen die Wirksamkeit des Lichtschutzsystems nicht beeinträchtigen.

Sicherheitsabstand

Eine gefahrbringende Maschinenbewegung muss angehalten werden, bevor eine Verletzung des Menschen erfolgen kann. Zwischen Lichtvorhang und Gefahrstelle muss ein Sicherheitsabstand eingehalten werden.

Wenn keine C-Norm mit anderen Anforderungen vorliegt, berechnet sich der Mindestabstand zum Gefahrbereich gemäß EN 999 nach folgender Formel:

$S = (K * T) + C$

Dabei ist:

S der Mindestabstand in Millimetern, gemessen vom Gefahrbereich zum Schutzfeld (bzw. Erkennungspunkt, zur Erkennungslinie, zur Erkennungsebene)

K ein Parameter in Millimetern je Millisekunde, abgeleitet von den Daten über Annäherungsgeschwindigkeit des Körpers oder von Körperteilen

T der Nachlauf des gesamten Systems in Millisekunden
t1: Ansprechzeit der Schutzeinrichtung
t2: Nachlaufzeit der Maschine

C ein zusätzlicher Abstand in Millimetern, der das Eindringen in den Gefahrbereich vor Auslösen der Schutzeinrichtung zugrunde legt

Die Werte für K und C sind abhängig von der Schutzfunktion (z.B. Hand- und Fingerschutz, Zugangssicherung), Auflösung und der Annäherungsrichtung.

Lichtvorhang in vertikaler Anordnung (max. Auflösung 40 mm)

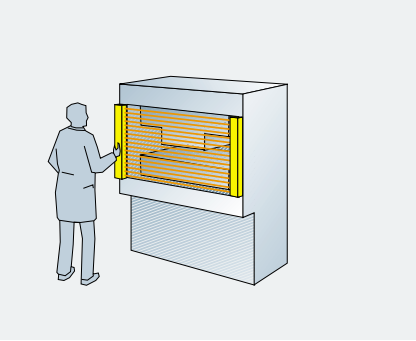


Bild 6/21

Ein Über-, Um- oder Untergreifen sowie das Hintertreten des Schutzfeldes muss ausgeschlossen werden. Dies kann durch zusätzliche mechanische Gitter oder durch die Kaskadierung von Host- und Guest-Lichtvorhängen geschehen.

Der minimale Sicherheitsabstand S berechnet sich nach

S = (K * T) + C

Mit

K = 2 mm/ms
C = 8 (d-14 mm),
jedoch nicht kleiner als 0.

Dabei ist

d = Auflösung des Lichtvorhangs in mm.

Wenn die Rechnung einen kleineren Wert als 100 mm ergibt, ist auf jeden Fall ein minimaler Abstand von 100 mm einzuhalten.

Wenn die Rechnung einen größeren Wert als 500 mm ergibt, kann diese mit K=1,6 mm/ms wiederholt werden. Auf jeden Fall ist ein minimaler Abstand von 500 mm einzuhalten.

Ist der Abstand zwischen Lichtvorhang und Maschine größer als 75 mm, muss ein Hintertretschutz (z.B. durch einen waagrecht angeordneten Lichtvorhang) angebracht werden.

Lichtvorhang in vertikaler Anordnung (Auflösung 40 mm ≤ 70 mm)

Der minimale Sicherheitsabstand S berechnet sich nach

S = (K * T) + C

Mit

K = 1,6 mm/ms

C = 850 mm

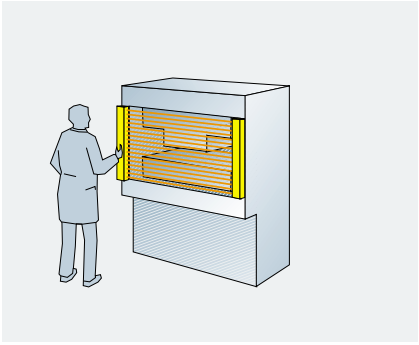


Bild 6/22

Mehrstrahlige Lichtgitter in vertikaler Anordnung zur Zugangssicherung

Ein Über-, Um- oder Untergreifen sowie das Hintertreten des Schutzfeldes muss ausgeschlossen werden. Dies kann durch zusätzliche mechanische Gitter oder durch die Kaskadierung von Host- und Guest-Lichtvorhängen geschehen.

Anzahl und Abstand der Lichtachsen hängen von der Risikobeurteilung bzw. von maschinenspezifischen Vorschriften ab.

Der minimale Sicherheitsabstand berechnet sich nach EN 999:

S = (K * T) + C

Mit

K = 1,6 mm/ms

C = 850 mm

Anzahl der Strahlen	Höhen über der Bezugsebene in mm
4	300, 600, 900, 1200
3	300, 700, 1100
2	400, 900

Lichtvorhänge in horizontaler Anordnung zur Gefahrbereichssicherung

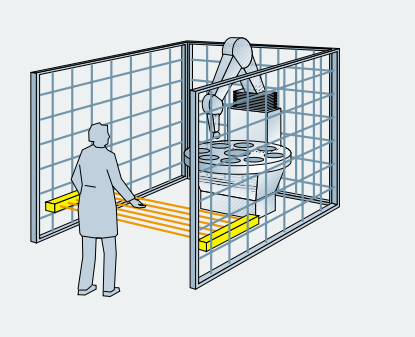


Bild 6/23

Bei der Gefahrbereichssicherung durch einen horizontal montierten Lichtvorhang darf die Höhe H des Schutzfeldes maximal 1000 mm betragen. Ist H größer als 300 mm (200 mm bei Anwesenheit von Kindern), kann das Schutzfeld unterkrochen werden. Dies muss bei der Risikobeurteilung berücksichtigt werden.

Die niedrigste zulässige Einbauhöhe hängt von der Auflösung des Lichtvorhangs ab, um sicherzustellen, dass das menschliche Bein bzw. Fußgelenk sicher erkannt wird.

$S = (K * T) + C$

$K = 1{,}6$ mm/ms

$C = (1200\ \text{mm} - 0{,}4 \times H)$

Dabei ist:

H = Höhe des Schutzfeldes über der Bezugsebene

$H_{max} = 1000$ mm

$H_{min} = 15\ (d - 50\ \text{mm})$

d = Auflösung des Lichtvorhangs

Wenn die Rechnung für C einen kleineren Wert als 850 mm ergibt, ist ein Minimalwert von C = 850 mm anzunehmen.

Generelle Beschreibung

Ein SIGUARD Lichtvorhang bzw. Lichtgitter besteht aus einem Sender und einem Empfänger, die einander gegenüber zu montieren sind. Abhängig von der Auflösung und Länge sind eine bestimmte Anzahl von Sende- und Empfangsdioden übereinander angeordnet. Die Infrarot-LEDs des Senders senden kurze Lichtpulse aus, die von den Empfängerdioden aufgefangen werden.

Eine Synchronisation zwischen Sender und Empfänger erfolgt ohne direkte elektrische Verbindung auf optischem Weg.

Je nach Applikation sind Lichtvorhänge mit unterschiedlichen Auflösungen notwendig.

Die Auflösung (Detektionsvermögen) eines Sicherheitslichtvorhanges ist diejenige Hindernisgröße, die an jeder Stelle des Schutzfeldes sicher erkannt wird und somit zum Abschaltbefehl führt.

Der Transceiver besteht aus einem Sender (Transmitter) und einen Empfänger (Receiver) in einem Gerät (Transceiver). Das Infrarotlicht der Sendediode wird über einen Spiegel zweimal um 90° reflektiert und gelangt so zu der Empfangsdiode des Transceivers zurück. Dadurch entsteht ein zweistrahliges Lichtgitter, das günstiger ist als ein herkömmliches Lichtgitter mit separatem Sender und Empfänger. Das Gerät besitzt fünf 5polige M12-Buchsen an der Frontscheibe, an die die Muting-Sensoren direkt angeschlossen werden können.

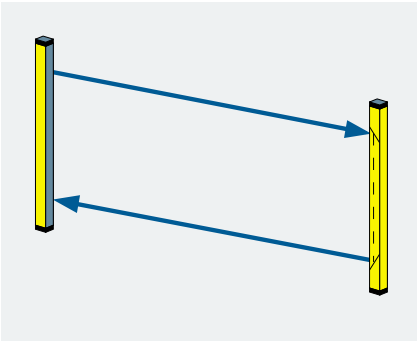


Bild 6/24
Transceiverprinzip

Bild 6/25
Transceiver

Sind alle Lichtachsen frei, schalten die OSSDs des Empfängers/Transceivers auf 24 V. Wird jedoch mindestens eine Lichtachse unterbrochen, schalten die Ausgänge sicher ab – z.B. bei einem Eingriff in die Gefahrenstelle.

Werden die Ausgänge der Lichtvorhänge abgeschaltet, kann dies über eine weiterführende Schaltung zum Sicheren Halt der gefahrbringenden Bewegung der Maschine genutzt werden. Die weiterführende Schaltung kann dabei ein SIGUARD Auswertegerät 3RG78 25/47 oder eine Sicherheitssteuerung (z.B. S7-400F/FH, S7-315F, SINUMERIK) sein.

Die SIGUARD Lichtvorhänge und Lichtgitter gibt es für Anwendungen der Sicherheitskategorie 2 und für höchste Sicherheitsansprüche für die Sicherheitskategorie 4 nach EN 954-1.

Testung und Überwachung von Lichtvorhängen

Bei Lichtvorhängen 3RG78 42/44 bzw. 3SF78 42/44 (Sicherheits-Kategorie 4) sind die Ausgänge redundant und selbstüberwachend, d.h. sie erkennen eine eventuelle Fehlfunktion sowie auftretende Fehler in der Außenbeschaltung (z.B. Quer- oder Kurzschluss).

Die SIGUARD Auswertegeräte 3RG78 25 und 3RG78 47 (außer 3RG78 47-4BB) führen einen automatischen Test durch, ohne den Prozess zu unterbrechen. Hierdurch wird ein gefahrbringender Ausfall (z.B. Verlust des Detektionsvermögens), der den bestimmungsgemäßen Betrieb beeinträchtigen würde, beim nächsten Testzyklus aufgedeckt.

Das Testsignal der Auswertegeräte kann auch für die Lichtvorhänge 3RG7841 Sicherheitskategorie 2 verwendet werden.

Host-/Guest-Kombinationen

Eine Kaskadierung von Geräten bedeutet eine Verlängerung der optischen Achse und somit der Schutzfeldhöhe, wobei durch ein flexibles Verbindungskabel zwischen Host- und Guestgerät gleichzeitig ein Schutz in horizontaler und vertikaler Ebene realisiert werden kann. Die Sicherheitsausgänge und die Prozessoraufgaben befinden sich im Hostgerät, so dass unabhängig vom Funktionspaket oder den Ausgängen die Guest-Geräte angeschlossen werden können. Das Standardkabel, mit dem das Host- und das Guestgerät verbunden werden kann, hat eine Länge von 300 mm. Die maximale Gesamtlänge einer Host-Guest-Kombination ist auf 240 Lichtstrahlen beschränkt.

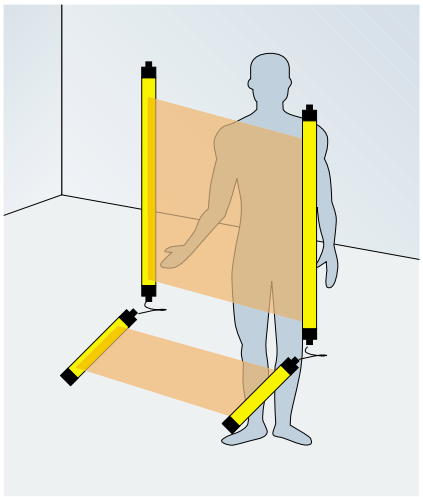


Bild 6/26
Host Guest

Software

Zur Visualisierung und Diagnose können sowohl die SIGUARD Lichtvorhänge Typ 2 und 4 als auch die Auswertegeräte über die serielle Schnittstelle an einen PC oder Laptop angeschlossen werden.

Die Diagnosesoftware für Lichtvorhänge visualisiert die Zustände der einzelnen Lichtstrahlen und erlaubt so eine einfache Ein- und Ausrichtung der Geräte. Außerdem erlaubt die Software eine Aufzeichnung dieser Daten während des laufenden Betriebs, um so zum Beispiel sporadisch auftretende Fehler eingrenzen zu können.

Bild 6/27
Bildschirmdarstellung Diagnosesoftware für Lichtvorhänge

Die Software für die Auswertegeräte bietet die oben genannten Möglichkeiten der Signalvisualisierung und -aufzeichnung für die SIGUARD Auswertegeräte. Das Diagnosekabel wird dazu einfach an die Klinkenbuchse des Geräts angeschlossen. Die Software erkennt automatisch die Gerätevariante und visualisiert die Zustände aller Ein- und Ausgänge.

Bild 6/28
Bildschirmdarstellung Diagnosesoftware für Auswertegeräte

Zubehör

Um Anbau, Justage, Inbetriebnahme und Störungssuche zu erleichtern, steht ein praxisgerechtes Zubehörprogramm, von Befestigungssäulen, Umlenkspiegelsäulen, Umlenkspiegeln, Halterungen und Laserausrichthilfen zur Verfügung. Die Befestigungssäulen und Umlenkspiegelsäulen erlauben die einfache Bodenmontage der Lichtvorhänge, Lichtgitter und Transceiver. Durch die spezielle Konstruktion können die Säulen nach Verschraubung am Boden zur exakten Ausrichtung der Lichtstrahlen justiert werden.

Mit den Laserausrichthilfen kann dieser Vorgang problemlos durchgeführt werden.

Anschlussvarianten

Die Lichtvorhänge, Lichtgitter und Transceiver sind in folgenden Anschlussvarianten lieferbar:

- Transistorausgang mit Kabelverschraubung
  Der Anwender führt die Versorgungsleitung durch eine Kabelverschraubung in der Endkappe der Geräte und schließt diese an Schraubklemmen in der Anschlusskappe an. Beim Sender wird nur die Versorgungsspannung zugeführt, Empfänger und Transceiver haben zusätzlich die beiden Sicherheits-Schaltausgänge OSSD1 und OSSD2 sowie weitere Signalein- und -ausgänge.

- Relaisausgänge mit Hirschmann-Anschluss
  Der Empfänger/Transceiver hat 2 Relais-Ausgänge und einen Anschluss für einen Hirschmann-Stecker in der Endkappe. Die Relaisausgänge mit Hirschmann-Anschluss sind für das Schalten von Schutzkleinspannungen bis 42 V AC/DC geeignet.
  Der Sender hat wie bei der Transistorvariante keine eigenen Ausgänge, besitzt aber ebenfalls für den Anschluss an das Maschinen-Interface einen Hirschmann-Anschluss. Die entsprechende Leitungsdose inklusive der Crimpkontakte bzw. komplette Anschlusskabel in verschiedenen Längen stehen als Zubehör in gerader oder gewinkelter Ausführung zur Verfügung.

- Maschinen-Interface mit ASIsafe-Anschluss
  Für den Sender steht ein 3poliger und für den Empfänger/Transceiver ein 5poliger M12-Stecker in den Endkappen für den Anschluss an das AS-Interface zur Verfügung. Ein geeignetes Koppelmodul gibt es als Zubehör, so dass das Gerät über ein Standard M12-Verlängerungskabel mit 1:1-Verbindung angeschlossen werden kann. Um eine Busadresse zu sparen, besteht die Möglichkeit einen Sender mit Kabelverschraubung oder Hirschmann-Stecker mit einem Empfänger mit ASIsafe-Anschluss zu kombinieren.

Funktionen

Funktionspakete bei integrierter Auswertung

Bei den SIGUARD Lichtvorhängen und Lichtgittern 3RG7842 der Kategorie 4 sowie den SIGUARD Lichtvorhängen 3RG78 41 der Kategorie 2 sind Funktionen wie Anlauf-/Wiederanlaufsperre, Schützkontrolle oder Muting nur in Verbindung mit einem Auswertegerät 3RG78 25 bzw. 3RG7847 möglich.

Die SIGUARD Lichtvorhänge und Lichtgitter 3RG7844 der Kategorie 4 stellen eine Ergänzung zu dem vorhandenen Produktspektrum dar und sind in vier Funktionspaketen erhältlich, in denen folgende Funktionen in die Geräte integriert sind. Das heisst ein Auswertegerät ist zur Realisierung dieser Funktionen nicht mehr erforderlich:

- Funktionspaket „Standard“: Anlauf-/Wiederanlaufsperre, Multi-Scan, Schützkontrolle, zwei Übertragungskanäle, sowie einen optionalen 2-kanaligen kontaktbehafteten Sicherheitskreis.

- Funktionspaket „Blanking“: wie das Funktionspaket „Standard“ und zusätzlich die Funktionen Fixed Blanking, Floating Blanking und Reduced Resolution

- Funktionspaket „Muting“: wie das Funktionspaket „Standard“ und zusätzlich die Funktion Muting, um die Schutzeinrichtung bestimmungsgemäß zeitlich begrenzt zu überbrücken.

- Funktionspaket Taktsteuerung: wie das Funktionspaket „Standard“ und zusätzlich die Funktion Taktsteuerung, um mit der Schutzeinrichtung nicht nur zu schützen, sondern auch sicherheitsrelevant zu steuern.

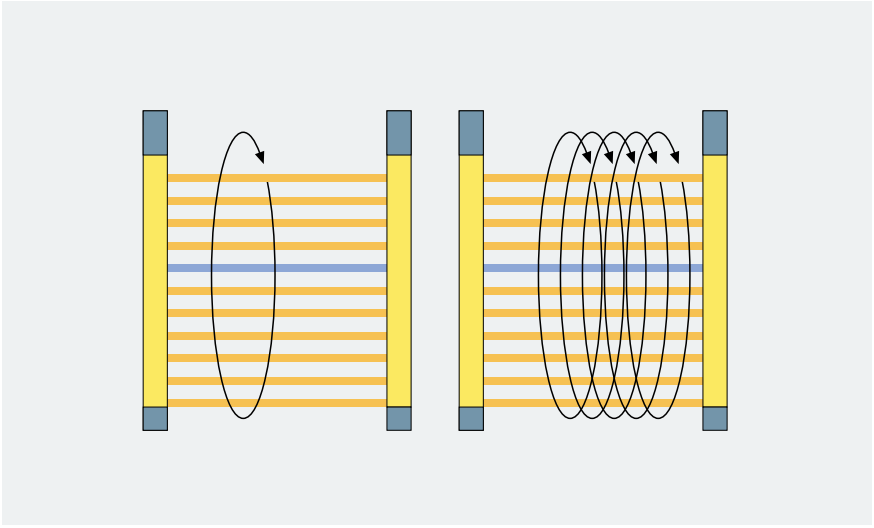


Bild 6/29
Multi-Scan

Erhöhung der Störfestigkeit gegen starkes Fremdlicht (Multi-Scan)

Werden Störungen durch starkes Fremdlicht bei rauen Umgebungsbedingungen zum Beispiel durch Stroboskoplampen oder Schweißroboter erwartet, ist es oft günstiger, bei Strahlunterbrechung zuerst zu warten, ob die Unterbrechung fortbesteht, bevor die Ausgänge abgeschaltet werden.

Besteht die Strahlunterbrechung nicht mehr, wurde diese evtl. durch die Umgebungsbedingungen ausgelöst und eine Abschaltung der Anlage ist nicht erforderlich.

Besteht die Strahlunterbrechung weiterhin, muss von einer Gefährdung ausgegangen werden und die Anlage wird abgeschaltet. Die Verfügbarkeit der Anlage wird auf diese Weise erhöht, wobei jedoch die Reaktionszeit und damit der Sicherheitsabstand vergrößert werden.

Wird Multi-Scan-Mode verwendet, schaltet der Empfänger bzw. Transceiver in den AUS-Zustand, sobald bei einer definierten Anzahl auf einander folgender Scans die Lichtstrahlen unterbrochen sind.

Übertragungskanäle

Die SIGUARD Lichtvorhänge, Lichtgitter und Transceiver 3RG784 und 3SF784 sind mit zwei unterschiedlichen Übertragungskanälen ausgestattet. Um das übertragene Infrarotlicht vom Umgebungslicht zu unterscheiden und um eine Beeinflussung von z.B. Warnlichtern von vorbeifahrenden Staplern oder Schweißfunken zu vermeiden, erfolgt die Übertragung in Impulspaketen.

Wenn sich zwei Schutzfelder einer Maschine direkt nebeneinander befinden und die Gefahr besteht, dass z.B. Strahlen vom Sender 1 auf den Empfänger 2 auftreffen, können zwei verschiedene Übertragungskanäle gewählt werden. Die Umstellung der Übertragungskanäle muss sowohl im Sender als auch im Empfänger erfolgen, damit sich die beiden entsprechenden Geräte erkennen.

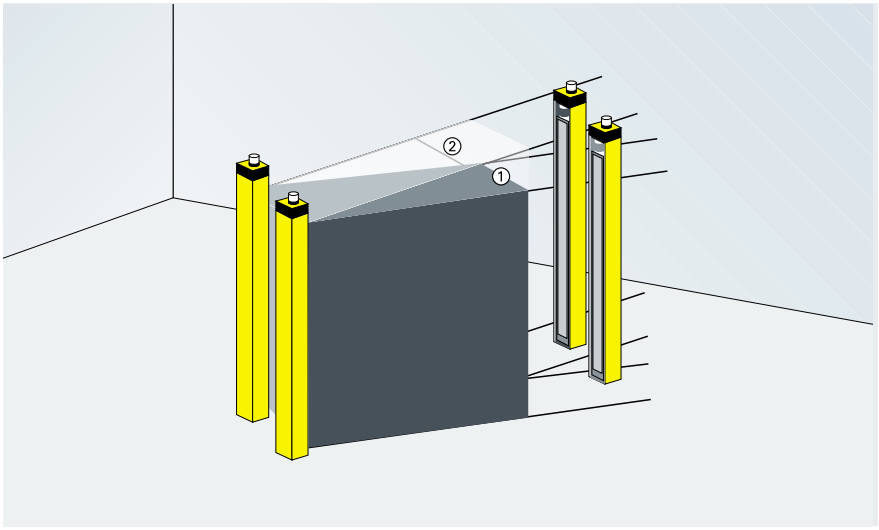


Bild 6/30
Übertragungskanäle

Anlauf-/Wiederanlaufsperre

Um zu verhindern, dass nach Auslösen und anschließendem wieder freiem Schutzfeld die Anlage sofort wiederanläuft, kann die Anlauf-/Wiederanlaufsperrenfunktion aktiviert werden. Erst wenn eine Start-Taste gedrückt und wieder losgelassen wird, schaltet der Empfänger bzw. der Transceiver in den EIN-Zustand. Das Drücken und Loslassen der Starttaste muss in einem Zeitfenster von 0,1 bis 4 Sekunden erfolgen.

Für Zugangssicherung ist die Verwendung der Anlauf-/Wiederanlaufsperre zwingend vorgeschrieben, da nur der Zutritt zur Gefahrzone, nicht aber der Bereich zwischen dem Schutzfeld und der gefahrbringenden Bewegung überwacht wird.

Das Befehlsgerät zur Freigabe der Anlauf-/Wiederanlaufsperre muss so montiert werden,

- dass der Gefahrenbereich vom Befehlsgerät aus gut einzusehen ist und
- das Befehlsgerät aus dem Gefahrenbereich heraus nicht bedient werden kann

Schützkontrolle

Die Schützkontrolle dient der Überwachung der dem Lichtvorhang nachgeschalteten Schütze, Relais oder Ventile. Schaltelemente mit zwangsgeführten Rückführkontakten sind hierfür Voraussetzung.

Bei dynamischer Schützkontrolle wird überprüft, ob nach der Freigabe der Rückführkreis innerhalb von 300 ms geöffnet hat und nach dem Abschalten der OSSD innerhalb von 300 ms wieder geschlossen ist. Ist das nicht der Fall, nimmt der Freigabekreis den AUS-Zustand wieder an.

Blanking-Funktionen

Es gibt drei verschiedene Blanking-Funktionen, die je nach Applikation ausgewählt werden können:

- Fixed Blanking für die Ausblendung von festen, sich nicht bewegenden Objekten
- Floating Blanking für bewegliche Objekte, die sich immer im Schutzfeld befinden
- Reduced Resolution für bewegliche Objekte im Schutzfeld, die zeitweise das Schutzfeld verlassen können

Die Konfigurierung erfolgt je nach Ausblendungsart über Teach-In mit Hilfe des SafetyKeys oder über DIP-Schalter in der Anschlusskappe. Auf das Mitführen und das Anschliessen eines PCs an eine Programmierschnittstelle kann verzichtet werden.

Fixed Blanking

Befinden sich dauerhaft nicht bewegliche Objekte im Schutzfeld des Lichtvorhangs, kann die Funktion „Fixed Blanking" eingesetzt werden. Wird diese Funktion nicht verwendet, würde der Lichtvorhang abschalten, weil nicht alle vom Sender ausgesandten Strahlen beim Empfänger ankommen würden.

Fixed Blanking ist an beliebiger Stelle des Lichtvorhangs möglich, wobei die Anzahl der ausgeblendeten Strahlen unbeschränkt ist. Der erste Strahl nach dem Anzeigenfeld kann nicht ausgeblendet werden, da es sich hierbei um den Synchronisationsstrahl zwischen Sender und Empfänger handelt.

Das ausgeblendete Objekt wird vom Lichtvorhang permanent überwacht: Der Lichtvorhang kontrolliert, ob sich das Objekt genau an der Stelle befindet, an der es eingelernt wurde. Wird das Objekt entfernt, schaltet der Lichtvorhang die Anlage ab, da ansonsten ein Sicherheitsrisiko durch die ausgeblendeten Lichtstrahlen entstehen würde.

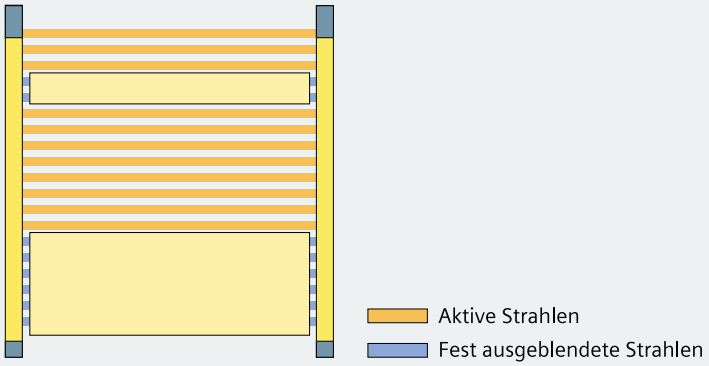


Bild 6/31
Fixed Blanking

Floating Blanking

Befinden sich dauerhaft bewegliche Objekte im Bereich des Lichtvorhangs, kann die Funktion Floating Blanking eingesetzt werden. Bei Floating Blanking können mehrere Objekte gleichzeitig ausgeblendet werden. Die Anzahl der gleitend ausblendbaren Strahlen ist unbeschränkt.

Das gleitend ausgeblendete Objekt wird permanent überwacht: Der Lichtvorhang kontrolliert, ob sich das Objekt dauerhaft im Bereich des Lichtvorhangs befindet.

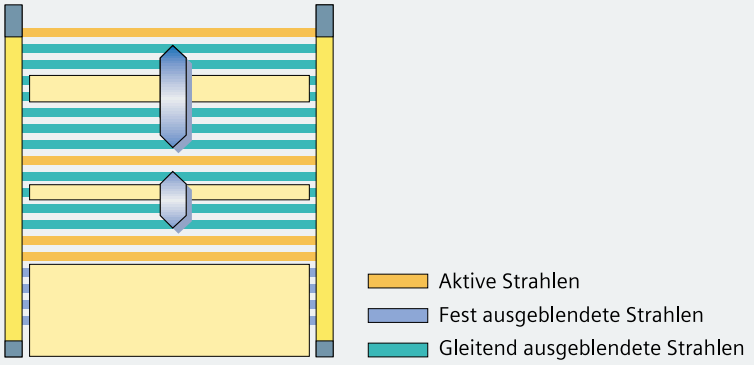


Bild 6/32
Floating Blanking

Reduzierte Auflösung

Befinden sich bewegliche Objekte nicht dauerhaft im Schutzfeld des Lichtvorhangs, kann die Funktion Reduced Resolution eingesetzt werden. Die permanente Überwachung des Objekts wird im Gegensatz zum Floating Blanking nicht durchgeführt. Es muss also kein Strahl unterbrochen sein, aber es können je nach Wahl der Strahlreduzierung mehrere Strahlen unterbrochen werden.

Bei Verwendung der Funktion „Reduced Resolution“ verändert sich die effektive Auflösung des Lichtvorhangs. Der Sicherheitsabstand muss mit der effektiven Auflösung neu berechnet werden.

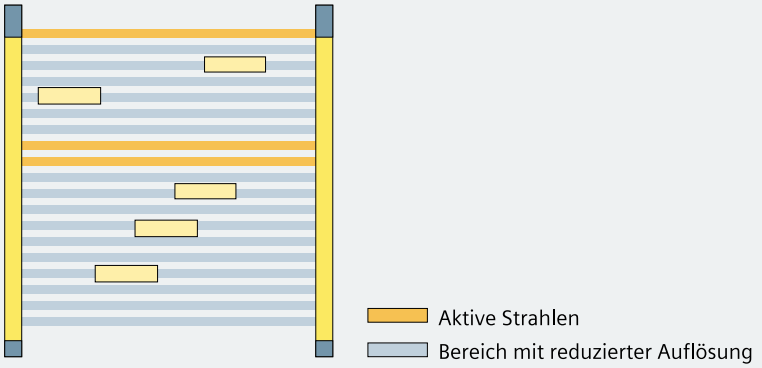


Bild 6/33
Reduced Resolution

Mutingfunktionen

Bei vertikaler Anordnung dienen Lichtvorhänge, Lichtgitter und Transceiver oft als Zugangssicherung. Mit zusätzlichen Sensorsignalen kann die Schutzwirkung unterdrückt werden, um z.B. Materialtransport in oder aus der Gefahrenzone zu transportieren. Das Schutzfeld wird temporär unterdrückt und nach Durchfahrt des Transportgutes wieder aufgehoben. Es muss gewährleistet sein, dass keine Person während des Mutingvorgangs in den Gefahrenbereich eintreten kann.

Durch die Anzahl der angeschlossenen Sensoren bzw. durch die Reihenfolge der Muting-Signale erkennen die Geräte automatisch den Muting-Mode „Sequenziell Muting“, wenn die Eingänge M1 bis M4 belegt sind und 2-Sensor-Parallel-Muting, wenn die Signale M2 und M3 belegt sind (Siehe Bild 6/34 und Bild 6/35). Die SIGUARD Lichtvorhänge, Lichtgitter und Transceiver 3RG78 44 bzw. 3SF 78 44 besitzen zusätzlich die Muting-Funktionen „3-Sensor-Richtungs-Muting“ und „4-SensorParallel-Muting“.

4-Sensor Sequenziell-Muting

Wenn das Material, das in den Gefahrenbereich transportiert werden soll, immer die gleichen Abmessungen hat und kein Platzmangel besteht, wird bevorzugt sequenzielles Muting eingesetzt. Beim sequenziellem Muting werden vier Mutingsensoren angeschlossen, deren Aktivierung in einer vorgegebenen Reihenfolge stattfinden muss, um den Muting-Vorgang auszulösen. Die Aktivierung kann sowohl in der Reihenfolge M1, M2, M3, M4 als auch in der Reihenfolge M4, M3, M2, M1 erfolgen. Das Transportgut muss lang genug sein, da kurzzeitig alle 4 Sensoren gleichzeitig aktiviert sein müssen. Das Sequenziell Muting wird korrekt beendet, wenn der dritte aktivierte Muting-Sensor nicht mehr aktiviert wird.

Mit der Software SafetyLab kann eine Mutingvariante gewählt werden, bei der die zweite Muting-Sequenz schon eingeleitet werden kann, auch wenn die erste noch nicht abgeschlossen ist. (Sequenziell Muting mit zwei Objekten). Diese Variante spart Zeit und damit auch Kosten in der Produktion des Anwenders.

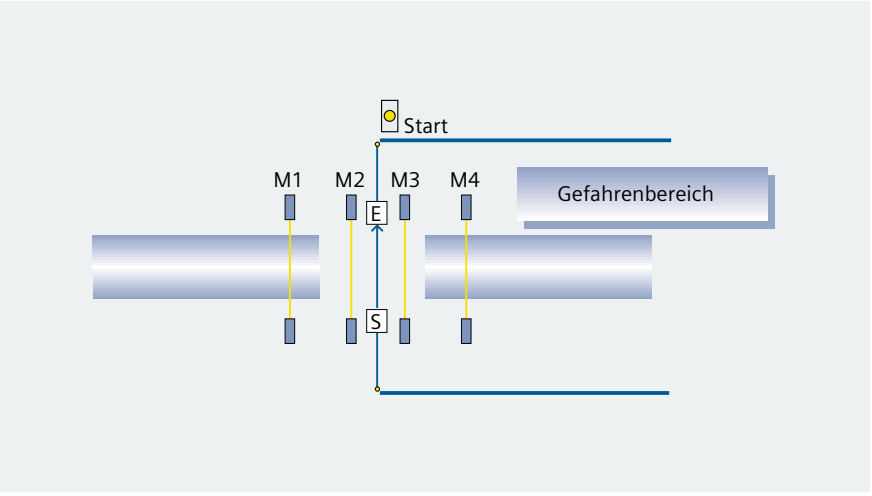


Bild 6/34
4 Sensor Sequenziell Muting

2-Sensor-Parallel-Muting

Parallel-Muting wird bevorzugt in solchen Anlagen eingesetzt, bei denen die Abmessungen des Transportgutes nicht konstant sind oder der Platzbedarf gering gehalten werden muss. Es kann mit zwei Mutingsensoren eingesetzt werden, deren Strahlen sich hinter dem Schutzfeld im Gefahrenbereich kreuzen.

Parallel-Muting wird dann eingeleitet, wenn die beiden Signale M2 und M3 gleichzeitig schalten, ohne dass vorher oder gleichzeitig M1 und M4 aktiviert bzw. angeschlossen wurden. Das 2-Sensor Parallel-Muting kann mit geringem Aufwand durchgeführt werden, da nur zwei Muting-Sensoren notwendig sind, und es besteht die Möglichkeit, innerhalb der Muting-Strecke vorwärts und rückwärts zu fahren.

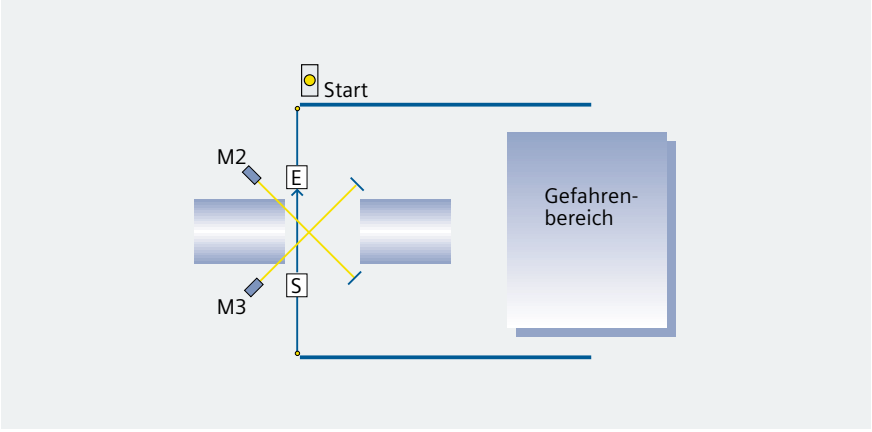


Bild 6/35
2 Sensor Parallel Muting

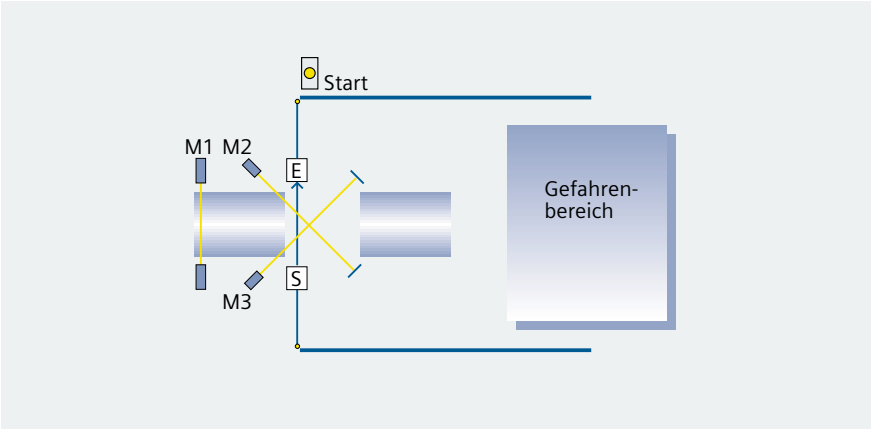


Bild 6/36
3 Sensor Richtungsmuting

3-Sensor-Richtungs-Muting

Das 3-Sensor-Richtungs-Muting ist ähnlich aufgebaut wie das 2-Sensor-Parallel-Muting. Der Transport des Materials durch den Lichtvorhang ist nur in einer Richtung möglich. Um die Muting-Funktion auszulösen, muss zuerst der Muting-Sensor M1 aktiviert werden, anschließend die beiden Muting-Sensoren M2 und M3. Sind die Wege der Muting-Sensoren M2 und M3 unterbrochen, ist eine Aktivierung des Sensors M1 nicht mehr erforderlich.

4-Sensor Parallel-Muting

Ist das Transportgut zu klein, um von 4 sequenziell angeordneten Sensoren gleichzeitig erkannt zu werden, und bietet die Applikation keinen Platz, um das Lichtschrankenkreuz des 2-Sensor Parallel Muting zu realisieren, bietet sich 4-Sensor Parallel-Muting z.B. unter Verwendung von Lichttastern an.

Das 4-Sensor Parallel-Muting entspricht funktionell dem 2-Sensor Parallel-Muting, allerdings wird das Aktivierungssignal aus jeweils zwei Sensorpaaren gewonnen. Wenn die Sensoren M2 mit M3 oder M1 mit M4 aktiviert werden, wird Muting eingeleitet.

Muting-Restart

Fällt z.B. die Spannungsversorgung aus, während das Transportgut die Muting-Sensoren passiert, wird die gültige Muting-Sequenz unterbrochen. Ist die Versorgungsspannung wieder vorhanden, wird der Mutingvorgang nicht automatisch fortgeführt, da die erwartete Muting-Sequenz nicht geliefert wird.

Um das Transportgut aus dem Bereich der Muting-Sensoren zu entfernen, kann ein integrierter Freifahr-Modus über die Starttaste erfolgen. Der Lichtvorhang versucht aus den Muting-Sensoren eine gültige Muting-Sequenz zu finden. Wenn das gelingt, beendet der Muting-Leuchtmelder das Blinken und leuchtet konstant. Gelingt dies nicht, muss die Starttaste so lange gehalten werden, bis die Muting-Strecke komplett freigefahren ist.

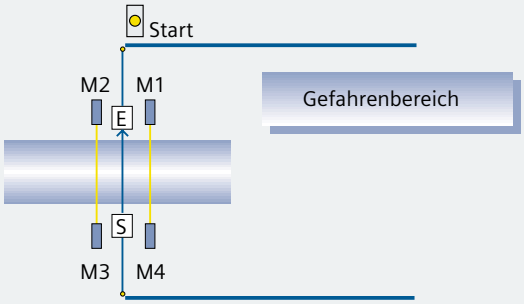


Bild 6/37
4 Sensor Parallel Muting

Auslösen der Maschinenbewegung durch den Lichtvorhang (Taktsteuerung)

Muss ein- oder zweimal in das Schutzfeld des Lichtvorhangs eingegriffen werden (z.B. zum Einlegen bzw. Entnehmen von Werkstücken), ist die optionale Funktion Taktsteuerung zu wählen. Die SIGUARD Lichtvorhänge, Lichtgitter und Transceiver 3RG78 44, Funktionspaket Taktsteuerung und entsprechende SIGUARD Auswertegeräte 3RG78 47 haben diese Funktionalität integriert und ermöglichen damit einen schnelleren und produktiveren Betrieb der Maschine.

6.3 SIGUARD Lichtschranken

Relevante Normen

- EN 61 496-1, -2, IEC 61 496-1, -2 (Anforderungen für berührungslos wirkende Schutzsysteme)
- EN 999 (u.a. Berechnung der Sicherheitsabstände)
- EN 954-1 (Sicherheit von Maschinen, sicherheitsbezogene Teile von Steuerungen)

Bild 6/38
SIGUARD Lichtschranken 3RG78 2

SIGUARD Lichtschranken

- sind aktive optoelektronische Schutzeinrichtungen (AOPD) und entsprechen Kategorie 2 (3RG78 23) bzw. 4 (3RG78 24) nach der Norm EN 61496-1, -2.
- sind EG-baumustergeprüft
- schützen das Bedienpersonal an oder in der Nähe von gefährlichen Maschinen
- wirken berührungslos
- sind im Vergleich zu mechanischen Systemen (z.B. Trittmatten) verschleißfrei

Voraussetzungen hierfür sind:

- die richtige Montage
- die korrekte Einbindung in die Maschinensteuerung

Hinweise hierzu finden Sie in diesem Kapitel und in den Betriebsanleitungen zu den jeweiligen Geräten.

Die Geräte sind EG-baumustergeprüft (TÜV Product Service in Zusammenarbeit mit dem Berufgenossenschaftlichen Institut für Arbeitssicherheit BIA).

Merkmale

Lichtschranken 3RG78 23 für Kategorie 2:

Reichweiten 0 bis 150 m
Schutzart IP65
Anschluss über M12-Steckverbinder
Integrierte Optikheizung

Lichtschranken 3RG78 24 für Kategorie 4:

Reichweite 0 bis 60 m
Schutzart IP65
Frequenzmoduliertes Infrarotlicht
Integrierte Verschmutzungskontrolle über LED
Integrierte Optikheizung
Hohe mechanische und chemische Widerstandsfähigkeit durch Glasoptik

Auswertegerät 3RG78 25 für Kategorie 2:

Anlauf- und Wiederanlaufsperre
Schützkontrolle
Potenzialfreie Sicherheitsausgänge
Separierte Meldeausgänge als pnp-Transistorausgänge
Permanent zyklische Testung
Keine Unterbrechung der Betriebsfunktion beim Test
Reihenschaltung von bis zu 6 Lichtschrankenpaaren

Mutingfunktionen für Lichschranken der Kategorie 2 und 4 unter Verwendung der Auswertengeräte 3RG78 47

Beispiele für Anwendungsbereiche

Lichtschranken in der Sicherheitskategorie 2:

- Kraftbetriebene Türen oder Tore
- Palletierer
- Regalgassen
- Umlaufpaternoster
- Hubbühnen
- Gefahrenbereich in der Fördertechnik

Lichtschranken in der Sicherheitskategorie 4:

- Setzmaschinen
- Verpackungsmaschinen
- Lagereinrichtungen
- Kunststoff- und Gummiindustrie
- Holzbearbeitungsmaschinen

Absicherungs-/Schutzfeldhöhen

Die Absicherungshöhen und die Anzahl der Lichtstrahlen werden durch die Anforderungen des jeweiligen kraftbetriebenen Arbeitsmittels, den gültigen Unfallverhütungsvorschriften, der EN 999 oder durch eine Risikoanalyse nach EN 954-1 festgelegt. Gebräuchliche Absicherungshöhen nach EN 999 gemäß Tabelle in Bild 6/39.

Einsatzbedingungen

Die Schutzfunktion der Schutzeinrichtung ist gegeben, wenn folgende Voraussetzungen erfüllt sind:

- Die Steuerung der Maschine oder Anlage muss elektrisch beeinflussbar sein.
- Ein Schaltbefehl muss zu einem unmittelbaren Abschalten der Maschine oder Anlage führen.
- Die angeschlossenen Lichtschranken müssen so angeordnet sein, dass ein Eindringen in den Gefahrenbereich nur durch die volle Abdeckung mindestens eines Lichtbündels möglich ist.
- Für den Einsatz und Aufbau der Sicherheitseinrichtungen gelten die einschlägigen gesetzlichen und behördlichen Bestimmungen der Berufsgenossenschaften und/oder der EU-Richtlinien für sicherheitstechnische Anforderungen an Maschinen und Anlagen.
- Die Lichtschranken sind so anzubringen, dass bei Unterbrechung mindestens eines Lichtbündels die Gefahrenstelle erst dann erreicht wird, wenn der gefährliche Zustand des KA (kraftbetriebenes Arbeitsmittel) aufgehoben ist. Voraussetzung hierfür ist, dass die erforderlichen Sicherheitsabstände gemäß EN 999 eingehalten werden.
- Alle Angaben der technischen Beschreibung und Betriebsanleitung, insbesondere die Abschnitte „Sicherheitshinweise“ und „Inbetriebnahme“ müssen unbedingt beachtet werden.
- Die Montage, Inbetriebnahme und Wartung der Geräte darf nur von qualifiziertem Fachpersonal durchgeführt werden.
- Elektrische Arbeiten dürfen nur von Elektro-Fachkräften durchgeführt werden.
- Einstellungen und Änderungen an der Sicherheitseinrichtung (z.B. Anordnung der Lichtstrahlen, Sicherheitsabstand etc.) dürfen nur von einem dazu autorisierten Sicherheitsbeauftragten vorgenommen werden.
- Reparaturen, insbesondere das Öffnen des Gehäuses, dürfen nur vom Hersteller oder einer vom Hersteller autorisierten Person vorgenommen werden.
- Sollten die Lichtschranken, z.B. aufgrund ihres Aufstellungsortes, allein nicht ausreichenden Schutz bieten, müssen zusätzliche mechanische Schutzeinrichtungen eingesetzt werden.
- Der Zugang zur Gefahrenstelle darf nur durch das Schutzfeld möglich sein (nicht umgehbar).
- Solange sich Personen im Gefahrenbereich aufhalten, darf die Anlage nicht anlaufen.
- Der START-Taster darf sich nicht aus dem Gefahrenbereich heraus betätigen lassen.

Sicherheitsabstand

Von der Unterbrechung der Lichtschranke bis zum Stillstand der Maschine verstreicht eine Verzögerungszeit. Die Lichtschranke muss deshalb so montiert werden, dass beim Eindringen in den Gefahrenbereich die Gefahrenstelle nicht erreicht werden kann, bevor die gefährliche Bewegung beendet ist.

Nach EN 999 ist der Sicherheitsabstand S zwischen der Schutzeinrichtung (Lichtschranke) und dem Gefahrenbereich nach folgender Formel festgelegt:

S = K x T + C

S Mindestsicherheitsabstand zwischen Lichtschranke und Gefahrenbereich in mm

K Greif- oder Annäherungsgeschwindigkeit in mm/s (Konstante)

T Verzögerungszeit zwischen Unterbrechung des Lichtstrahls und Stillstand der Maschine in s, bestehend aus:
t1: Ansprechzeit der Schutzeinrichtung in s
t2: Nachlaufzeit der Maschine in s

C Sicherheitskonstante (zusätzlicher Abstand in mm)

Achtung:

Es sind grundsätzlich die Normen EN 294 und EN 999 maßgebend.

Anzahl der Lichtstrahlen und Höhe der Lichtstrahlen über Bezugsebene nach EN 999

Anzahl der Lichtstrahlen	Anzahl der Lichtstrahlen über Bezugsebene in mm	Strahlenabstand S in mm
4	300, 600, 900, 1200	300
3	300, 700, 1100	400
2	400, 900	500
1	750	

Bild 6/39
Höhe und Sicherheitsabstände der Strahlen (in allen Anwendungsfällen ist die EN 999 zu beachten)

Abstand zu spiegelnden Flächen

Spiegelnde Flächen, die sich innerhalb der Sende- und Empfangskeule der Lichtschranken befinden, können zum Umspiegeln und dadurch zum Nichterkennen eines Hindernisses führen. Deshalb muss ein Mindestabstand von spiegelnden Gegenständen zur optischen Achse eingehalten werden. Dieser Abstand ist abhängig vom Öffnungswinkel der Lichtschranke und dem Abstand von Sender und Empfänger.

Systemaufbau

Die SIGUARD Lichtschranken sind berührungslos wirkende Schutzeinrichtungen der Kategorie 2 bzw. 4 nach EN 954-1. Sie sind zur Absicherung von Gefahrenbereichen und Gefahrenstellen an Maschinen, die ein Verletzungsrisiko bergen, vorgesehen. Bei bestimmungsgemäßer Verwendung veranlassen sie die Maschine, einen ungefährlichen Zustand einzunehmen, bevor eine Person verletzt werden kann.

Das komplette Sicherheitssystem besteht für die Sicherheitskategorie 2 aus einer Auswerteeinheit und den zugehörigen Lichtschranken. An das Auswertegerät 3RG78 25 können bis zu 6 Lichtschrankenpaare in Reihe geschaltet werden.
Das System für die Sicherheitskategorie 4 besteht aus zwei Lichtschranken.

Beide Systeme arbeiten zusammen mit den Auswertegeräten 3RG78 47, um Funktionen wie z.B. Muting zu realisieren.

Die Auswerteeinheiten sind in Verbindung mit den zugehörigen Sicherheitslichtschranken als selbstüberwachende Komponenten entsprechend EN 954-1, Kategorie 2 bzw. 4, ausgeführt. Sie stellen das Bindeglied zwischen den Lichtschranken und der Maschinensteuerung dar und stellen alle für den Betrieb der Lichtschranken erforderlichen Schnittstellen inklusive der Energieversorgung zur Verfügung.

Die sichere Funktion des Gesamtsystems wird nach dem Einschalten der Betriebsspannung (Anlauftestung nach „power on“) und nach Testaufforderung (Betätigung eines START-Tasters) geprüft. Zusätzlich wird während des Betriebs eine zyklische Überprüfung durchgeführt, um die internen Funktionen zu testen.

Bild 6/40
SIGUARD Auswertegerät 3RG78 25

Anlauf-/Wiederanlaufsperre

Um zu verhindern, dass nach Auslösen und anschließendem wieder freiem Schutzfeld die Anlage sofort wiederanläuft, kann die Anlauf-/Wiederanlaufsperrenfunktion aktiviert werden. Erst wenn eine Start-Taste gedrückt und wieder losgelassen wird, schaltet der Empfänger bzw. der Transceiver in den EIN-Zustand. Das Drücken und Loslassen der Starttaste muss in einem Zeitfenster von 0,1 bis 4 Sekunden erfolgen.

Für Zugangssicherung ist die Verwendung der Anlauf-/Wiederanlaufsperre zwingend vorgeschrieben, da nur der Zutritt zur Gefahrzone, nicht aber der Bereich zwischen dem Schutzfeld und der gefahrbringenden Bewegung überwacht wird.

Das Befehlsgerät zur Freigabe der Anlauf-/Wiederanlaufsperre muss so montiert werden,

- dass der Gefahrenbereich vom Befehlsgerät aus gut einzusehen ist und
- das Befehlsgerät aus dem Gefahrenbereich heraus nicht bedient werden kann

Schützkontrolle

Die Schützkontrolle dient der Überwachung der nachgeschalteten Schütze, Relais oder Ventile. Schaltelemente mit zwangsgeführten Rückführkontakten sind hierfür Voraussetzung.

Bei dynamischer Schützkontrolle wird überprüft, ob nach der Freigabe der Rückführkreis innerhalb von 300 ms geöffnet hat und nach dem Abschalten der OSSD innerhalb von 300 ms wieder geschlossen ist. Ist das nicht der Fall, nimmt der Freigabekreis den AUS-Zustand wieder an.

Mutingfunktionen

Mit zusätzlichen Sensorsignalen kann die Schutzwirkung unterdrückt werden, um z.B. Materialtransport in oder aus der Gefahrenzone zu transportieren. Das Schutzfeld wird temporär unterdrückt und nach Durchfahrt des Transportgutes wieder aufgehoben. Es muss gewährleistet sein, dass keine Person während des Mutingvorgangs in den Gefahrenbereich eintreten kann.

Durch die Anzahl der angeschlossenen Sensoren bzw. durch die Reihenfolge der Muting-Signale erkennen die Geräte automatisch den Muting-Mode „Sequenziell Muting“, wenn die Eingänge M1 bis M4 belegt sind und 2-Sensor-Parallel-Muting, wenn die Signale M2 und M3 belegt sind (siehe Bild 6/41 bzw. 6/42).

4-Sensor Sequenziell-Muting

Wenn das Material, das in den Gefahrenbereich transportiert werden soll, immer die gleichen Abmessungen hat und kein Platzmangel besteht, wird bevorzugt sequenzielles Muting eingesetzt. Beim sequenziellen Muting werden vier Mutingsensoren angeschlossen, deren Aktivierung in einer vorgegebenen Reihenfolge stattfinden muss, um den Muting-Vorgang auszu-

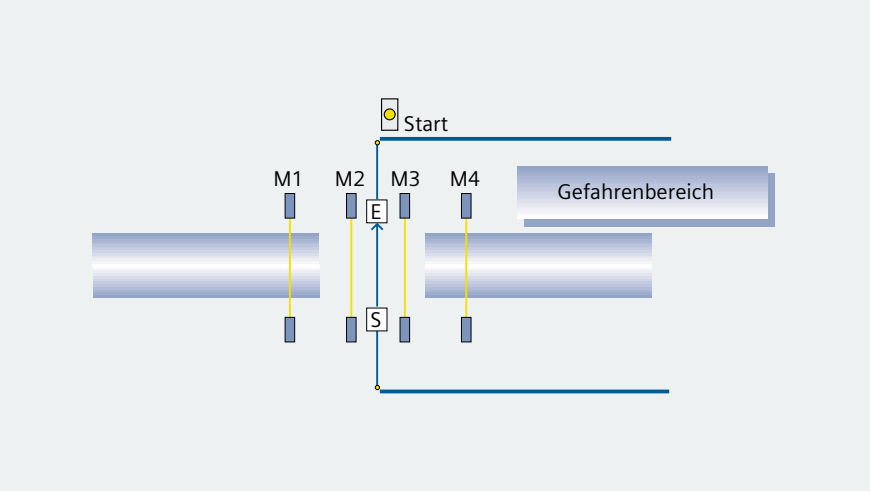


Bild 6/41
Sensor Sequenziell Muting

lösen. Die Aktivierung kann sowohl in der Reihenfolge M1, M2, M3, M4 als auch in der Reihenfolge M4, M3, M2, M1 erfolgen. Das Transportgut muss lang genug sein, da kurzzeitig alle 4 Sensoren gleichzeitig aktiviert sein müssen. Das Sequenziell Muting wird korrekt beendet, wenn der dritte aktivierte Muting-Sensor nicht mehr aktiviert wird.

2-Sensor-Parallel-Muting

Parallel-Muting wird bevorzugt in solchen Anlagen eingesetzt, bei denen die Abmessungen des Transportgutes nicht konstant sind oder der Platzbedarf gering gehalten werden muss.

Es kann mit zwei Mutingsensoren eingesetzt werden, deren Strahlen sich hinter dem Schutzfeld im Gefahrenbereich kreuzen.

Parallel-Muting wird dann eingeleitet, wenn die beiden Signale M2 und M3 gleichzeitig schalten, ohne dass vorher oder gleichzeitig M1 und M4 aktiviert bzw. angeschlossen wurden. Das 2-Sensor Parallel-Muting kann mit geringem Aufwand durchgeführt werden, da nur zwei Muting-Sensoren notwendig sind, und es besteht die Möglichkeit, innerhalb der Muting-Strecke vorwärts und rückwärts zu fahren.

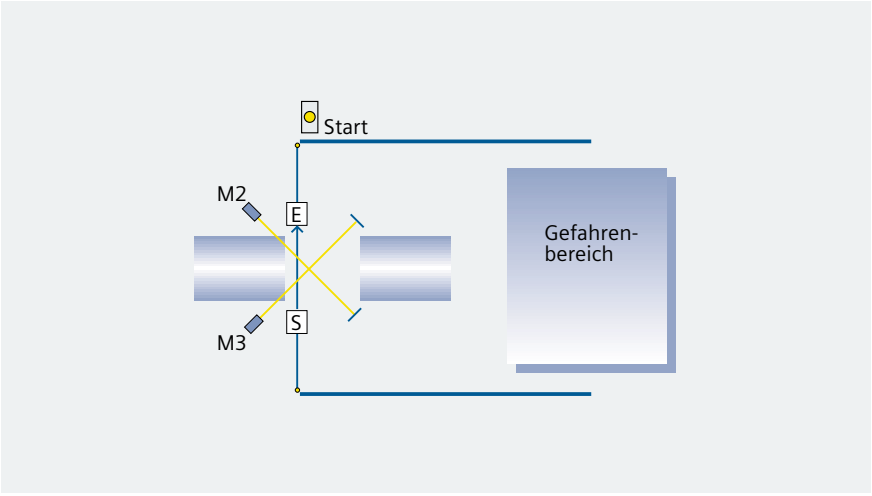


Bild 6/42
Sensor Parallel Muting

6.4 SIGUARD Schaltleisten

Übersicht

Eine Schaltleiste ist eine mechanisch betätigte Schutzeinrichtung, die die Berührung durch eine Person oder eines Körperteils sicher erkennt

Optische und elektrische Kopplung von Sender und Empfänger

Sicheres Erkennen einer Unterbrechung des Lichtstrahls, der Beeinflussung durch Fremdlicht oder eines Fehlers an elektrischen Bauteilen

Automatische Anpassung der Leistung des Senders an die Länge der Schaltleiste

Erhöhte Verfügbarkeit durch Kompensation von Alterungseffekten, Feuchtigkeit und Verschmutzung

Abschalt- und Nachlaufwege unabhängig von der Länge des Profils

Merkmale

- Kein Verkleben oder Vorkonfektionieren notwendig
- Kein technisches Know-how oder Spezialwerkzeug notwendig
- Problemloser Einbau des Systems vor Ort
- Flexible Planung bis kurz vor den Einbau
- Kostengünstige Lagerhaltung
- Minimierung der Stillstandzeiten

Anwendungsbereiche

Maschinen- und Anlagenbau
- Schutzhauben von Maschinen
- Fahrerlose Transportsysteme
- Hubtische
- Waschportale
- Hebebühnen
- Automatische Handhabungsgeräte

Tür- und Torbereich
- Begrenzung der auftretenden Kräfte auf ein Hindernis
- Auswahl eines geeigneten Profils
- Berücksichtigung des Betätigungswinkels bei Falttoren

Fahrzeugbau
- Begrenzung der auftretenden Kräfte auf ein Hindernis
- Auswahl eines geeigneten Profils
- Zuverlässigkeit auch bei hohen Geschwindigkeiten
- Automatisch schließende Tore
- Automatisch schließende Fenster

Produktfamilie/Produktgruppen

SIGUARD Schaltleisten 3RG78 5 sind für Kategorie 4 nach EN 954-1 von der BG zugelassen. Die entsprechende Fehlersicherheit wird mit dem zugehörigen Auswertegerät erreicht.

Das System besteht aus
- einem Auswertegerät,
- einer Montageleiste,
- einer Sensorleiste, über die die Abschaltfunktion realisiert wird,
- einem Sender und einem Empfänger, die auf optischer Basis die Schaltleiste überwacht

Aufbau

Sender- und Empfängereinheit werden links und rechts in den Hohlraum des Gummiprofils gesteckt. Das Gummiprofil kann individuell und kundenspezifisch vor Ort zugeschnitten werden und ist beständig gegen äußere Einflüsse wie z.B. Ozon, Öle, Lösungsmittel, Säure und Kraftstoffe.

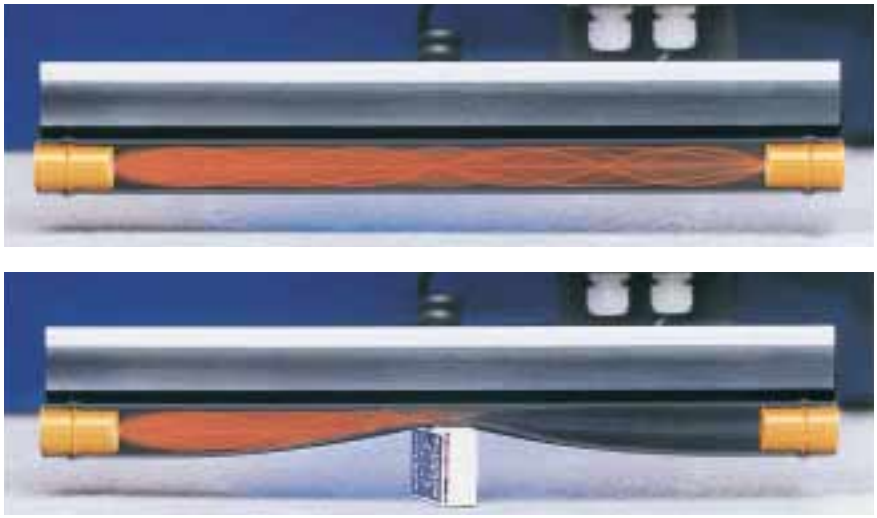
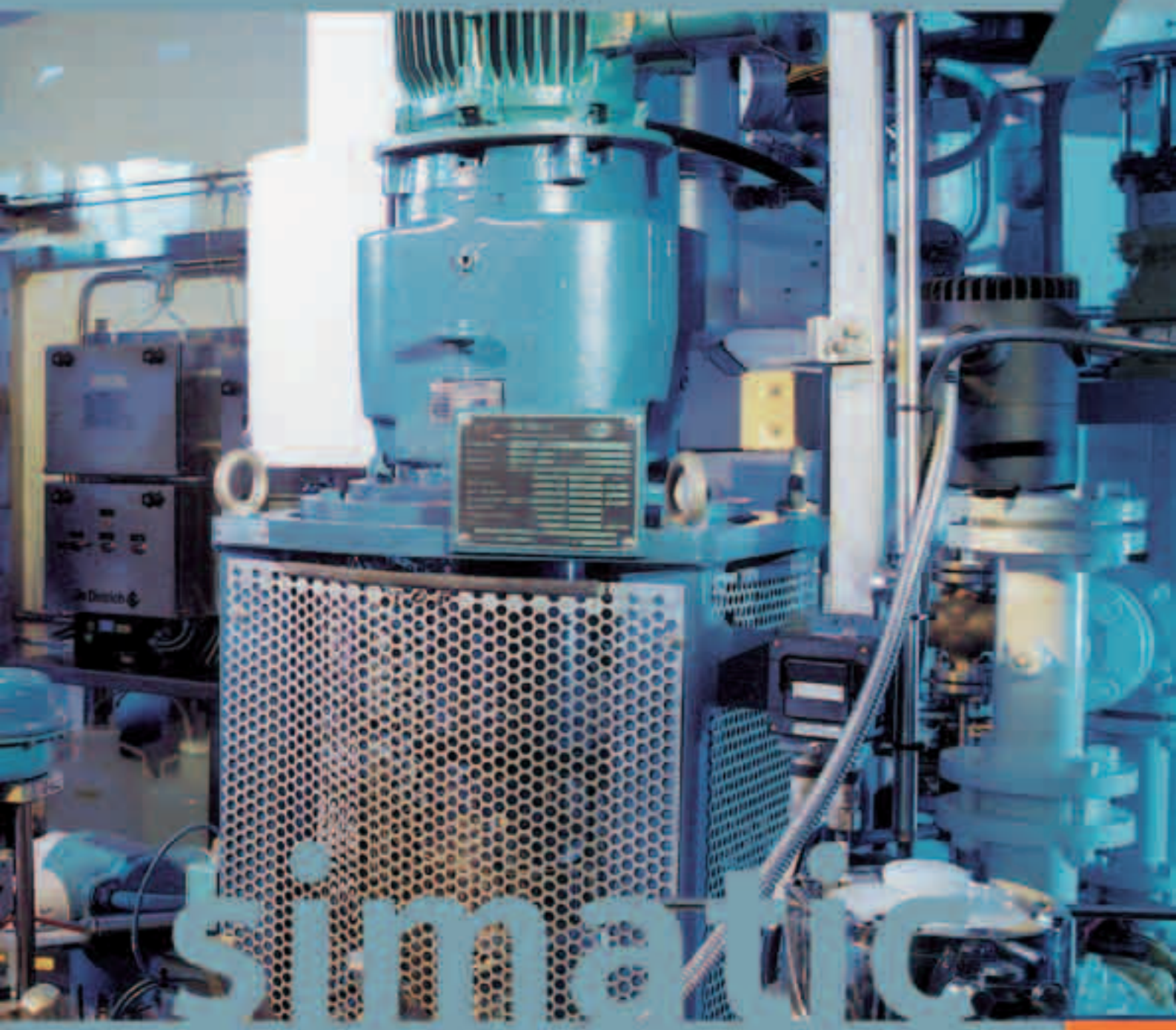


Bild 6/43
Funktionsprinzip der SIGUARD Schaltleisten

7.1 Übersicht
7.2 Merkmale
7.3 Anwendungsbereich
7.4 Produktgruppe/Produktfamilie
7.5 Engineering
7.6 Aufbau
7.7 Funktionen
7.8 Beispiele
7.9 Technische Daten

Fehlersichere Steuerungen



7 Fehlersichere Steuerungen SIMATIC Safety Integrated

7.1 Übersicht

Zunehmende Bedeutung der Sicherheitstechnik bei Steuerungen

Unfälle und Schäden als Folge von Fehlern in Maschinen oder Anlagen sind soweit wie möglich zu vermeiden. Weltweit wird deshalb die Gesetzgebung zur Sicherheit am Arbeitsplatz und zum Schutz der Umwelt immer strenger. Dabei werden heute oft unterschiedliche Produkte und Systeme für sicherheitsgerichtete Funktionen (Elektromechanik) und Standardaufgaben (klassische SPS) eingesetzt. Durch konventionelle Verdrahtung und den Einsatz spezieller Sicherheitsbusse erhöhen sich mit steigender Komplexität der Automatisierungsaufgabe

- einerseits die Verdrahtungskosten und
- andererseits der Engineeringaufwand.

Die Fehlerdiagnose kann länger dauern und die Verfügbarkeit der Gesamtanlage nimmt ab.

Deshalb übertragen Maschinenhersteller und Anlagenbetreiber den Automatisierungskomponenten zunehmend auch sicherheitsrelevante Aufgaben. Der Schutz von Menschen, Maschinen und Umwelt hängt also von der fehlerfreien Funktion von Automatisierungssystemen ab. An sicherheitsgerichtete elektronische Systeme werden daher die gleichen hohen Anforderungen wie an sicherheitsgerichtete elektromechanische Komponenten gestellt. Es müssen sowohl systematische als auch zufällige Fehler beherrscht werden.

Standardautomatisierung und Sicherheitstechnik in einem Gesamtsystem

Bislang war es üblich, Sicherheits- und Standardaufgaben mit unterschiedlichen Systemen zu lösen. Die Folge waren Systembrüche und doppelter Aufwand. Bei SIMATIC Safety Integrated werden Standardautomatisierung und Sicherheitstechnik zu einem innovativen Gesamtsystem integriert. Vorhandenes SIMATIC-Know-how und Kenntnisse der Sicherheitstechnik reichen aus, um sicherheitsgerichtete Aufgaben mit SIMATIC zu lösen.

Bewährte Sicherheitstechnik mit SIMATIC

Seit mehr als 20 Jahren ist Siemens in der Sicherheitstechnik etabliert und hat seit dieser Zeit bei fehlersicheren Steuerungen viele Innovationen vorangetrieben. In vielen Bereichen hat Siemens mit SIMATIC Safety Integrated Pionierarbeit geleistet, wie z.B.

- Erste fehlersichere Speicherprogrammierbare Steuerung – 1980
- Erster fehlersicherer PROFIBUS-Master mit PROFIsafe – 1999

Weiterhin arbeitet Siemens aktiv in nationalen und internationalen Gremien an der Gestaltung von Normen und Richtlinien mit wie z.B. ISO, NAM, DKE, IEC etc.

Was bedeutet SIMATIC Safety Integrated für den Anwender?

Die Standardautomatisierung ist durch den Wechsel hin zur intelligenten Steuerung und Dezentralisierung wesentlich flexiber und offener geworden. Damit stieg die Produktivität ihrer Maschinen und Anlagen erheblich. Noch effizienter wird ihre Automatisierung, wenn auch die Sicherheitstechnik diesem Trend konsequent folgt und sich nahtlos in die Standardautomatisierung integriert. Das bedeutet:

- Vorhandenes STEP7 Know-how vom Engineering bis zur Instandhaltung nutzen.
- Vorhandene PROFIBUS-Netzwerkstrukturen auch für sichere Kommunikation einsetzen.
- Vorhandene Komponenten und Infrastruktur so weit als möglich auch für Sicherheitstechnik verwenden.

7.2 Merkmale

Integriertes Gesamtsystem

Durch die Integration sicherheitstechnischer Funktionen in die Automatisierungswelt von Totally Integrated Automation wachsen die Standardautomatisierung und die Sicherheitsautomatisierung zu einem durchgängigen Gesamtsystem zusammen.

SIMATIC Safety Integrated umfasst die fehlersicheren Steuerungen SIMATIC sowie Peripherie und Engineering innerhalb des Produktspektrums von Safety Integrated. Beim Auftreten eines Fehlers kann die Steuerung oder ein Teilprozess in einen sicheren Zustand überführt und dort gehalten werden. Diese fehlersicheren Steuerungen basieren auf bewährten SIMATIC Standard-SPS.

Der PROFIBUS wurde für die sicherheitsgerichtete Kommunikation um das herstellerunabhängige PROFIsafe-Profil erweitert. Somit sind sicherheitsgerichtete und Standard-Kommunikation über nur ein Standard-PROFIBUS-Kabel möglich.

Das Engineering für die Standard- und die Sicherheitsfunktionen der fehlersicheren SIMATIC-Steuerungen erfolgt mit den gleichen Projektier- und Programmierwerkzeugen (STEP® 7).

Somit wird in einer SIMATIC-Steuerung die Sicherheitstechnik nahtlos in die Standardautomation integriert. Dadurch wird auch die Bedienung der Gesamtanlage durch das Bedienpersonal vereinfacht. Und neben den Engineeringkosten sinken zusätzlich die Aufwändungen für das Training. Ein weiterer Vorteil ist, dass umfangreiche Diagnose sicherheitsgerichteter Signale über Standard Panels und HMI-Geräte ohne Umwege auslesbar ist.

Durch den feingranularen Aufbau der fehlersicheren Peripherie muss Sicherheitstechnik nur dort eingesetzt werden, wo sie notwendig ist. Ein kombinierter Aufbau mit Sicherheitskomponenten und Standardkomponenten ist einfach möglich; ebenfalls die Koexistenz sicherheitsgerichteter und nicht-sicherheitsgerichteter Programme in einer Steuerung sowie auf einem gemeinsamen Bussystem.

Auch die Anbindung von fehlersicheren Feldbusgeräten anderer Hersteller ist mit Hilfe des PROFIBUS und dem herstellerunabhängigen PROFIsafe-Profil einfach realisierbar.

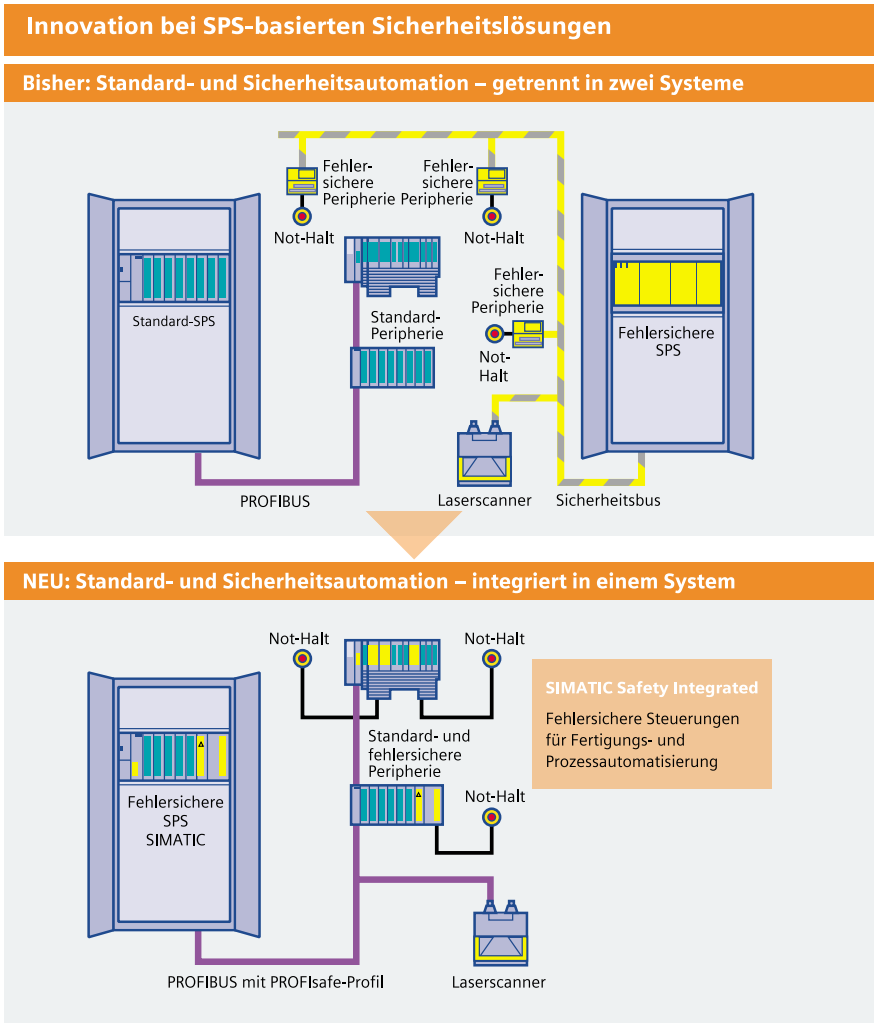


Bild 7/1
Innovation bei SPS-basierten Sicherheitslösungen

Vergleich bisherige / neue Lösung

Bisherige sicherheitsgerichtete SPS-Lösungen erfordern zwei unterschiedliche Steuerungen und bei dezentralen Lösungen einen zusätzlichen fehlersicheren Bus. Standard- und fehlersichere Feldgeräte müssen getrennt aufgebaut werden. Zum Auslesen sicherheitsgerichteter Signale müssen zusätzliche HMI-Geräte installiert werden.

Die neue und bereits weltweit bewährte Lösung mit SIMATIC Safety Integrated benötigt nur eine Steuerung mit einheitlichem Engineering und dem Standard-PROFIBUS mit dem PROFIsafe-Profil. Standard- und sicherheitsgerichtete Automatisierung wachsen auch bei den Peripheriemodulen, den HMI-Geräten und den Sensoren zusammen. Bei Bedarf können die Systeme auch wie bisher getrennt aufgebaut werden. Aber auch in diesem Fall bleiben die Vorteile der einheitlichen Engineering-Werkzeuge sowie die Integration ohne neue Schnittstelle erhalten.

Die Vorteile im Überblick

Mit SIMATIC Safety Integrated profitieren:

- Maschinen- und Anlagenbauer z.B. durch Kosteneinsparungen bei Hardware.
- Anlagenbetreiber z.B. durch höhere Anlagenverfügbarkeit und hohe Flexibilität.

Im Einzelnen ergeben sich Vorteile im Vergleich sowohl zu einer proprietären Sicherheits-SPS als auch zu konventioneller Sicherheitstechnik.

Vorteile von SIMATIC Safety Integrated	gegenüber proprietärer Sicherheits-SPS	gegenüber konventioneller Sicherheitstechnik
Geringerer Aufwand für Engineering	• Nur ein Engineering Tool für die Erstellung von Standard- und Sicherheitsprogramm	• Einfaches Duplizieren einer Lösung durch Kopieren des Sicherheitsprogramms
	• Gemeinsame Datenhaltung für Standard- und Sicherheitsprogramm	• Höhere Flexibilität durch Programmierung statt Verdrahtung der Sicherheitslogik
	• Einheitliche Projektierung der Standard- und der sicherheitsgerichtete Komponenten und Kommunikation	
Einfachere und schnellere Inbetriebnahme	• Nur ein PROFIBUS-Kabel für die Standard- und sicherheitsgerichtete Kommunikation	• Einfache Modifizierung der Sicherheitslogik durch Programmänderungen mit automatischer Nachführung der Dokumentation
	• Gleiche Bedienphilosophie für Standard- und sicherheitsgerichtete Automatisierung	• Durchgängige Diagnose vom Sensorüber die Steuerung bis zum HMI-System
	• Alle Systemkomponenten aus einer Hand	
Effizientere Betriebsphase	• Kürzere Stillstandszeiten aufgrund durchgängiger Diagnose vom Sensor über die Steuerung bis zum HMI-System	
	• Ferndiagnose über Teleservice	
	• Erleichterte Ersatzteilhaltung durch Typen- und Teilereduzierung	

Tabelle:
Vorteile von SIMATIC Safety Integrated

7.3 Anwendungsbereich

Einsatz von SIMATIC Safety Integrated

Das Produktspektrum der fehlersicheren Steuerungen SIMATIC umfasst breit skalierbare Sicherheitslösungen sowohl für die Fertigungs- als auch für die Prozessautomatisierung.

- In der Fertigungsautomatisierung stehen Sicherheit und Schutz von Menschen und Maschinen im Vordergrund.
- In der Prozessautomatisierung muss vor allem die Systemverfügbarkeit aufrechterhalten werden. Gleichzeitig muss der Schutz vor unerwarteten Gefahren des Prozesses sichergestellt und das Risiko eines Un- oder Zwischenfalls entsprechend vermindert werden.

Die Erfüllung aller wichtigen Normen und Standards ermöglicht den weltweiten Einsatz von SIMATIC Safety Integrated zum Schutz von Mensch, Maschine und Umwelt.

Zuhause in allen Branchen

Die Einsatzschwerpunkte von SIMATIC Safety Integrated sind z.B. wie folgt:

- **Fertigungsautomatisierung**
  Automobilindustrie, Fördertechnik, Pressen, Be- und Verarbeitungsmaschinen, Werkzeugmaschinen, etc. Personentransport, z.B. Seilbahnen, Hebebühnen, Fahrgeschäfte, etc.

- **Prozessautomatisierung**
  Oil&Gas, Chemie, Pharma, Petrochemie, Raffinerien,
  Typische Applikationen:
  Brennersteuerungen, Emergency Shutdowns (ESD), Process Shutdowns (PSD) and Fire&Gas (F&G)

Besonders bei Mischanwendungen aus beiden Schwerpunktbranchen, in der Hybridindustrie, kommt die Durchgängigkeit von SIMATIC Safety Integrated, unter anderem bei Kommunikation und gemeinsamer Peripherie zum Tragen.

Zertifiziert nach allen wichtigen Normen

Die fehlersicheren Steuerungen SIMATIC erfüllen alle wichtigen Normen und Vorschriften und sind vom TÜV zertifiziert.

Fertigungsautomatisierung
- IEC 61508 (bis SIL 3)
- EN 954 (bis Kategorie 4)
- NFPA 79-2002 und NFPA 85
- UL 1998, UL 508 und UL 991

Zertifikat unter:
http://www4.ad.siemens.de/WW/view/de/17396090

Prozessautomatisierung
- IEC 61508 (bis SIL 3) und IEC 61511
- EN 954 (bis Kategorie 4)
- NFPA 79-2002
- ANSI/ISA S84, API 14C, BLRBAC

Zertifikat unter:
http://www4.ad.siemens.de/WW/view/de/17968956

PROFIBUS mit PROFIsafe ist als Bestandteil von SIMATIC Safety Integrated zertifiziert nach IEC 61508 (bis SIL 3), EN 954 (bis Kategorie 4), NFPA 79-2002, NFPA 85 und erfüllt damit höchste Anforderungen für die Fertigungs- und die Prozessindustrie. Und mit der Übertragungsvariante PA (IEC 1158-2) erweitert PROFIBUS DP die Durchgängigkeit dezentraler Automatisierung bis in die Prozesswelt. Die Peripheriebaugruppen erfüllen SIL 3 (nach IEC 61508) und Kategorie 4 (nach EN 954) und sind sowohl UL-gelistet als auch TÜV-zertifizeirt.

7.4 Produktgruppe/ Produktfamilie

SIMATIC Safety Integrated Familie

SIMATIC Safety Integrated bietet ein skalierbares Angebot an fehlersicheren Steuerungen für die Fertigungs- und Prozessautomatisierung, wobei eine gemeinsame Peripherie und Kommunikation verwendet werden.

Als fehlersichere Peripherie kommt die ET 200S, ET 200M und ET 200eco zum Einsatz. Der Anschluss der Peripherie erfolgt über PROFIBUS DP, die Kommunikation über das PROFIsafe-Profil.

SIMATIC Safety Integrated

Spektrum für die Fertigungsindustrie	Spektrum für die Prozessindustrie
Controller	
SIMATIC ET 200S F-CPU, S7-300F, S7-400F Skalierbares Angebot fehlersicherer Controller für alle Leistungsbereiche in der Fertigungsautomatisierung.	**SIMATIC S7-400FH** Sicherer, fehlertoleranter Controller für die Prozessautomatisierung
Engineering	
Die Programmierung erfolgt mit den STEP 7-Sprachen KOP und FUP und TÜV-zertifizierten Funktionsbausteinen von **S7 Distributed Safety**.	Die Projektierung der Sicherheitsfunktionen erfolgt mittels **Continuous Function Chart** (CFC) oder **SIMATIC Safety Matrix** (Cause&Effect-Matrix) via TÜV-zertifizierten Funktionsbausteinen von **S7 F Systems**.
Peripherie	
Die fehlersichere Peripherie ist einsetzbar in allen Industrien und unterstützt Sicherheitsfunktionen, wie z. B. Signaltest (Kurzschluss, Drahtbruch) sowie Diskrepanzüberwachung.	
ET 200eco Die dezentrale Blockperipherie in hoher Schutzart IP65/67 mit digitalem Eingabemodul für den schaltschranklosen Aufbau. **ET 200M** Die modulare Peripherie für hochkanalige Anwendungen mit digitalen Ein- und Ausgabebaugruppen sowie analogen Eingabebaugruppen. **ET 200S** Die feinmodulare Peripherie mit digitalen Ein- und Ausgabemodulen sowie fehlersicherem Motorstarter und Frequenzumrichter.	

Bild 7/2
SIMATIC Safety Integrated für die Fertigungs- und Prozessautomatisierung

Controller für die Fertigungsautomatisierung

Die folgenden F-CPUs stehen für die Fertigungsautomatisierung zur Verfügung:

- IM 151-7 F-CPU der ET 200S
- CPU 315F und CPU 317F der S7-300
- CPU 416F der S7-400

Diese CPUs basieren auf den jeweiligen Standard-CPUs, deren Hardware und Betriebssystem zur Abarbeitung von Sicherheitsprogrammen um verschiedene Schutzmechanismen erweitert wurde.

Die gesamte Programmierung des sicherheitsgerichteten Programms erfolgt mit STEP 7 in den Standard-Sprachen KOP und FUP.
Dazu ist das Optionspaket „S7 Distributed Safety" zusätzlich zu STEP 7 nötig.
"S7 Distributed Safety" unterstützt bei der Parametrierung der fehlersicheren Peripherie und bei der Programmierung durch vorgefertigte, zertifizierte Bausteine.

Bei der Bearbeitung nicht-sicherheitsgerichteter Programme bestehen keinerlei Einschränkungen hinsichtlich der Programmiersprache.

Bild 7/3
CPUs für die Fertigungsautomatisierung

Controller für die Prozessautomatisierung

Für den Einsatz in der Prozessindustrie stehen die hochverfügbaren CPUs 414H und CPU 417H mit nachladbaren Sicherheitsfunktionen der S7-400 zur Verfügung. Sicherheitsgerichtete Anwendungen in der Prozessindustrie erfordern ein spezielles Softwarepaket „S7 F-Systems". Mit einer CPU lassen sich fehlersichere Anwendungen bis SIL 3 lösen. "S7 F-Systems" unterstützt die Konfiguration der sicherheitsgerichteten Peripherie und die Programmierung der Logik.

Für erweiterte Systemverfügbarkeit können zwei CPUs verwendet werden, um Forderungen nach Fehlersicherheit und Hochverfügbarkeit zu erfüllen. Sehr einfach möglich ist auch die Einbindung in das Prozessleitsystem SIMATIC PCS 7. Dadurch ergeben sich folgende Vorteile:

- Ein Engineering System für Standard und fehlersichere Applikationen
- Homogene Integration der Sicherheitstechnik in das Automatisierungssystem (AS) von SIMATIC PCS 7
- Komfortable Visualisierung der Prozesswerte integriert in die Operator Station (OS) von SIMATIC PCS 7
- Automatische Einbindung der sicherheitsrelevanten Störungsmeldungen in die Prozessvisualisierung, mit gleichem Zeitstempel
- Keine aufwändige Kopplung zwischen Distributed Control System (DCS) und SIMATIC Safety Integrated, z.B. über Modbus

Die Projektierung der sicherheitsgerichteten Funktionen erfolgt in Continuous Function Chart (CFC). Zertifizierte Funktionsbausteine helfen bei der Projektierung und sparen somit Zeit und Geld ein.

Um die Projektierung der sicherheitsgerichteten Funktionen noch mehr zu vereinfachen, steht jetzt auch ein Projektierungstool zur Verfügung, das eine schnelle und fehlerfreie Konfiguration von Ursachen und Wirkungen im Prozess ermöglicht. Die SIMATIC Safety Matrix ist ein Projektierungstool für Prozesse, die Sicherheitsreaktionen auf definierte Zustände erfordern und sich mittels Cause&Effects-Matrix einfach projektieren lassen.

Bild 7/4
S7-400FH CPUs für die Prozessautomatisierung

Fehlersichere Peripherie

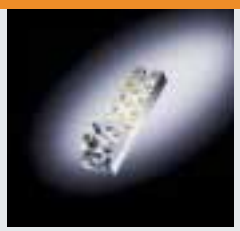
Für die Erweiterung der fehlersicheren CPUs für die Fertigungsautomatisierung stehen ET 200S, ET 200M und ET 200eco als fehlersichere Peripherie zur Verfügung. Die fehlersicheren CPUs 414H und 417H können um die fehlersichere Peripherie ET 200M und ET 200S erweitert werden.

Die fehlersichere ET 200M, ET 200S und ET 200eco erfüllen SIL 3 (nach IEC 61508) und Kategorie 4 (nach EN 954) und sind UL-gelistet und TÜV-zertifiziert. Der Anschluss der Peripherie erfolgt über PROFIBUS DP, die Kommunikation über das PROFIsafe-Profil.

Die fehlersichere Peripherie kann interne und externe Fehler diagnostizieren, ist intern redundant aufgebaut und führt eigene Selbsttests (z.B. Kurzschluss, Drahtbruch) durch. In einer ET 200S oder ET 200M können fehlersichere und Standard-Baugruppen auch in Kombination betrieben werden. Je nach Systemaufbau kann hierbei bis SIL 3 bzw. Kat. 4 erreicht werden. Die folgende Tabelle zeigt die Hauptmerkmale der verfügbaren fehlersicheren Peripherie.

Anforderung	Aufbau	Sicherheitsklasse Safety Integrated Level
Fehlersicher	Einfacher Aufbau mit einer CPU	bis SIL 3
Fehlersicher und Hochverfügbar	Redundanter Aufbau mit zwei CPUs	bis SIL 3

Tabelle:
Sicherheitsklassen bei den verschiedenen Aufbauvarianten

Peripherie	ET 200S	ET 200M	ET 200eco *)
			
Merkmal	Feinmodulare Peripherie mit bis zu 8 Kanälen pro Baugruppe in Schutzart IP20	Modulare S7-300 Peripherie für hochkanalige Anwendungen mit bis zu 24 Kanälen pro Baugruppe in Schutzart IP20	Digitale Blockperipherie in hoher Schutzart IP65/67
Digitaleingänge	Für den Anschluss digitaler Sensoren / Geber • 4/8 F-DI DC 24V	Für den Anschluss digitaler Sensoren / Geber • 24 F-DI DC 24V • 8 F-DI NAMUR	Für den Anschluss digitaler Sensoren / Geber • 4/8 F-DI DC 24V
Digitalausgänge	Für den Anschluss digitaler Aktoren / Lasten • 4 F-DO DC 24V/2A	Für den Anschluss digitaler Aktoren / Lasten • 10 F-DO DC 24V/2A • 8 F-DO DC 24V/2A (PM-sch.)	
Analogeingänge		Für den Anschluss analoger Sensoren / Geber • 6 F-AI 4-20 mA / 13 Bit	
Power Module	Zur Überwachung und Absicherung der Last- und Geberversorgungsspannungen • PM-D F DC 24 V • PM-E F PM • PM-E F PP		
Motorstarter	Die fehlersicheren Motorstarter besitzen neben einer Leistungsschalter-/ Schützkombination eine sichere elektronische Auswerteschaltung zur Fehlererkennung. Versagt im Not-Halt-Fall das zu schaltende Schütz, erkennt die Auswerte-Elektronik einen Fehler und schaltet den Leistungsschalter im Motorstarter sicherheitsgerichtet ab.		
Frequenzumrichter	Die fehlersicheren Frequenzumrichter ermöglichen folgende Sicherheitsfunktionen bei drehzahlgeregelten Asynchronmotoren: • Sicherer Halt, • Sichere Bremsrampe, • Sicher reduzierte Geschwindigkeit.		

*) nicht einsetzbar mit den CPUs 414H und 417H

Tabelle:
Gegenüberstellung der verschiedenen Peipherie-Familien

7.5 Engineering

Programmierung in der Fertigungsautomatisierung

Bei Verwendung des Softwarepakets „S7 Distributed Safety“ wird kein zusätzliches Programmier-Know-how benötigt. Denn die Programmierung der sicherheitsgerichteten Programme für die fehlersicheren CPUs erfolgt mit den gewohnten STEP7-Standardsprachen Kontaktplan (KOP) und Funktionsplan (FUP). Durch eine spezielle Vorgabe bei der Kompilierung wird sichergestellt, dass das vom Anwender erstellte Programm sicherheitsgerichtet abgearbeitet wird.

Zusätzlicher Bestandteil dieses Softwarepakets ist die F-Bibliothek mit vorgefertigten und vom TÜV abgenommenen Bausteinen für sicherheitsgerichtete Funktionen. Dazu zählen Funktionsbausteine, wie Not-Halt, Schutztür, 2-Hand-Bedienung, Muting bei Lichtvorhängen usw.

Außerdem unterstützt „S7 Distributed Safety“ den Vergleich von sicherheitsgerichteten Programmen. Schließlich wird mit dem generierten Programmausdruck die Abnahme der Anlage vereinfacht.

Für Brenneranwendungen steht ein Optionspaket mit zertifizierten Brenner-Bausteinen zur Verfügung.

Projektierung in der Prozessautomatisierung

“S7 F Systems“ dient zur Konfiguration der Hardware und Projektierung der sicherheitsgerichteten Prozessapplikation nach IEC 61511 und erweitert die S7-400FH Controller um Sicherheitsfunktionen. Es vereinfacht die Erstellung des Sicherheitsprogramms durch Bereitstellung einer F-Bibliothek mit vorgefertigten und TÜV-zertifizierten Bausteinen nach SIL 3 IEC 61508. Zusätzlich erleichtert es die Dokumentation des Sicherheitsprogramms, z.B. durch Verwaltung der Signaturen.

Die Projektierung des fehlersicheren Sicherheitsprogramms kann wahlweise mit CFC oder der Safety Matrix erfolgen.

CFC eignet sich besonders für Prozesse mit dynamischem Verhalten, z.B. in der Chemie, Petrochemie (Hydro-cracker). Mittels CFC können die zertifizierten Bausteine aus der F-Bibliothek von S7 F Systems oder dem optionalen Brennerpaket aufgerufen und verschaltet werden. Das optionale Brennerpaket enthält eine F-Bibliothek mit Bausteinen für industrielle Gas- und Ölbrenner. Die Bausteine sind vom TÜV nach EN 61508 SIL 3 und den TRD-Normen 411 und 412 für Thermo- und Dampfkessel zertifiziert.

Die Safety Matrix ist ein innovatives Projektierungs-Tool für Prozesse, die Sicherheitsreaktionen auf definierte Zustände erfordern und sich mittels Cause&Effects-Matrix einfach projektieren lassen. Die Cause&Effects-

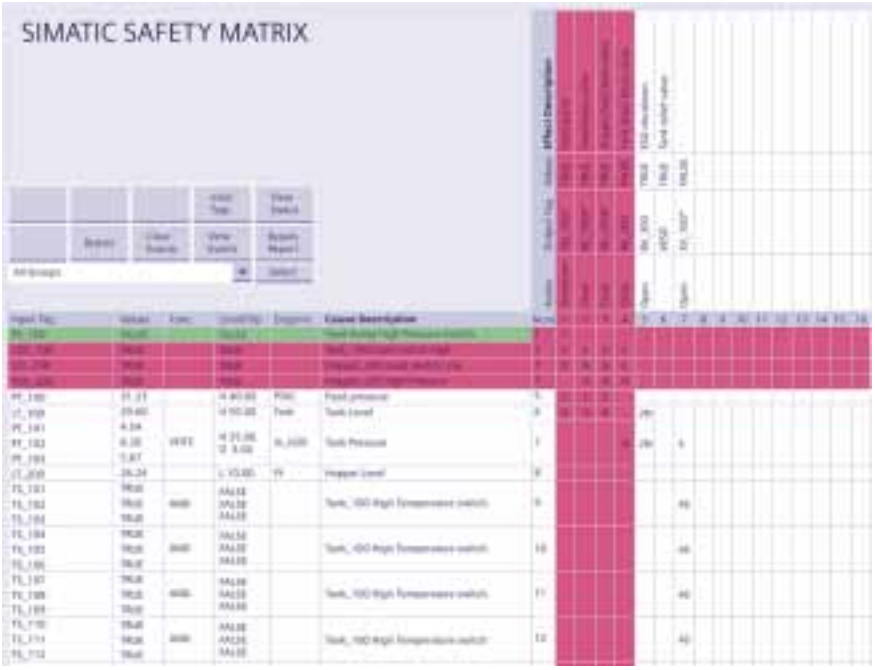


Bild 7/5
Beispiel der SIMATIC Safety Matrix für S7-400FH

Analyse ist Bestandteil der Risikoanalyse einer Anlage. Dabei entspricht die Spezifikation des Sicherheitsprogramms gleichzeitig den Eingabeparametern für die Safety Matrix. Nach erfolgreicher Eingabe leitet sich die Prüfspezifikation der Anlage ab. Mögliche Fehlerquellen lassen sich somit auf ein Minimum reduzieren.

Damit sind folgende Vorteile verbunden:

- Automatisches Erzeugen des sicherheitsgerichteten CFC-Projekts.
- Automatische Dokumentationserstellung nach Sicherheitsüberprüfungen.
- Automatische Generierung der Visualisierung und komfortable Darstellung der Safety Matrix an der Operator Station von SIMATIC PCS 7.
- Automatische Verwaltung von Projektversionen.
- Leichtes Ändern der Sicherheitsfunktion und einfaches Anpassen der Spezifikation im Testmodus inklusive Bypass-, Reset- und Override-Funktionen.

7.6 Aufbau

Realisierung der Sicherheitsfunktionen

Die Sicherheitsfunktionen werden durch das Sicherheitsprogramm in der CPU in Verbindung mit fehlersicheren Peripheriebaugruppen ausgeführt. Dabei können Standard-Peripherie und fehlersichere Peripherie auch kombiniert aufgebaut werden. Die erforderliche galvanische Trennung für SIL 3 bzw. Kat. 4 Anwendungen erfolgt bei der ET 200M mittels Trennbaugruppe bzw. bei der ET 200S durch den Aufbau von Lastkreisen mittels Powermodulen (PMs).

Sowohl die sicherheitsgerichtete als auch die Standard-Kommunikation zwischen Zentralbaugruppe und Peripherie (sicherheitsgerichtet oder Standard) erfolgen über PROFIBUS DP mit dem PROFIsafe-Profil.

Prinzip der Sicherheitsfunktion bei SIMATIC Safety Integrated

Zeitredundanz und Diversität statt struktureller Redundanz ist das Funktionsprinzip, mit dem sicherheitsgerichtete Eingangssignale diversitär und Zeit redundant verarbeitet werden.

In Bild 7/6 werden die Signale A, B parallel mit einer UND Verküpfung bzw. negiert mit einer ODER Verknüpfung verarbeitet. Die Ausgangssignale C und D werden danach miteinander verglichen. Wenn D ungleich dem Komplement von C ist, geht die CPU in Stop. Wenn der Vergleich erfolgreich ist, wird der Ausgang gesetzt.

Die CPU überprüft den ordnungsgemäßen Betrieb der Steuerung durch regelmäßige Selbsttests, Befehlstests sowie eine Programmablaufkontrolle.

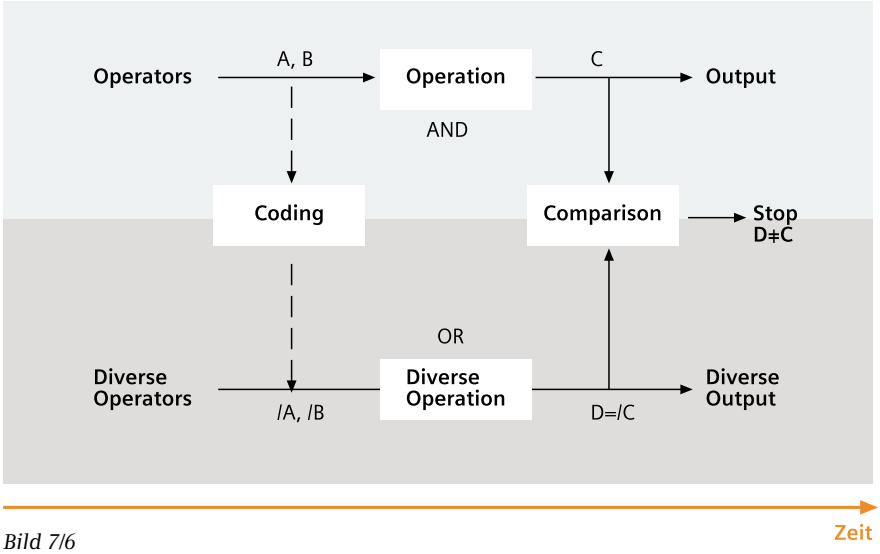


Bild 7/6
Sichere Datenübertragung durch Zeitredundanz und Diversität bei S7 F Systems

7.7 Funktionen

Funktionen der fehlersicheren Controller

Die fehlersicheren CPUs verfügen über folgende Eigenschaften:

- Umfangreiche Selbsttests und Eigendiagnose, um den fehlersicheren CPU-Zustand zu überprüfen.
- Neben dem fehlersicheren Programm kann auf einer CPU auch ein Standardprogramm ablaufen (Koexistenz), das keinen Einschränkungen unterliegt.
- Fehlersichere Kommunikation zwischen den CPUs.
- Gleiche Diagnose- und Meldefunktionen wie eine Standard SIMATIC S7-CPU.

Funktionen der fehlersichere Peripherie

Die fehlersichere Peripherie kann interne und externe Fehler diagnostizieren, ist intern redundant aufgebaut und führt eigene Selbsttests (z.B. Kurzschluss, Drahtbruch) durch. Das fehlersichere Abschalten erfolgt ohne zusätzliche Sicherheitsrelais. Ebenso wird die per Parametrierung vorgegebene Diskrepanzzeit von der Peripheriebaugruppe eigenständig überwacht.

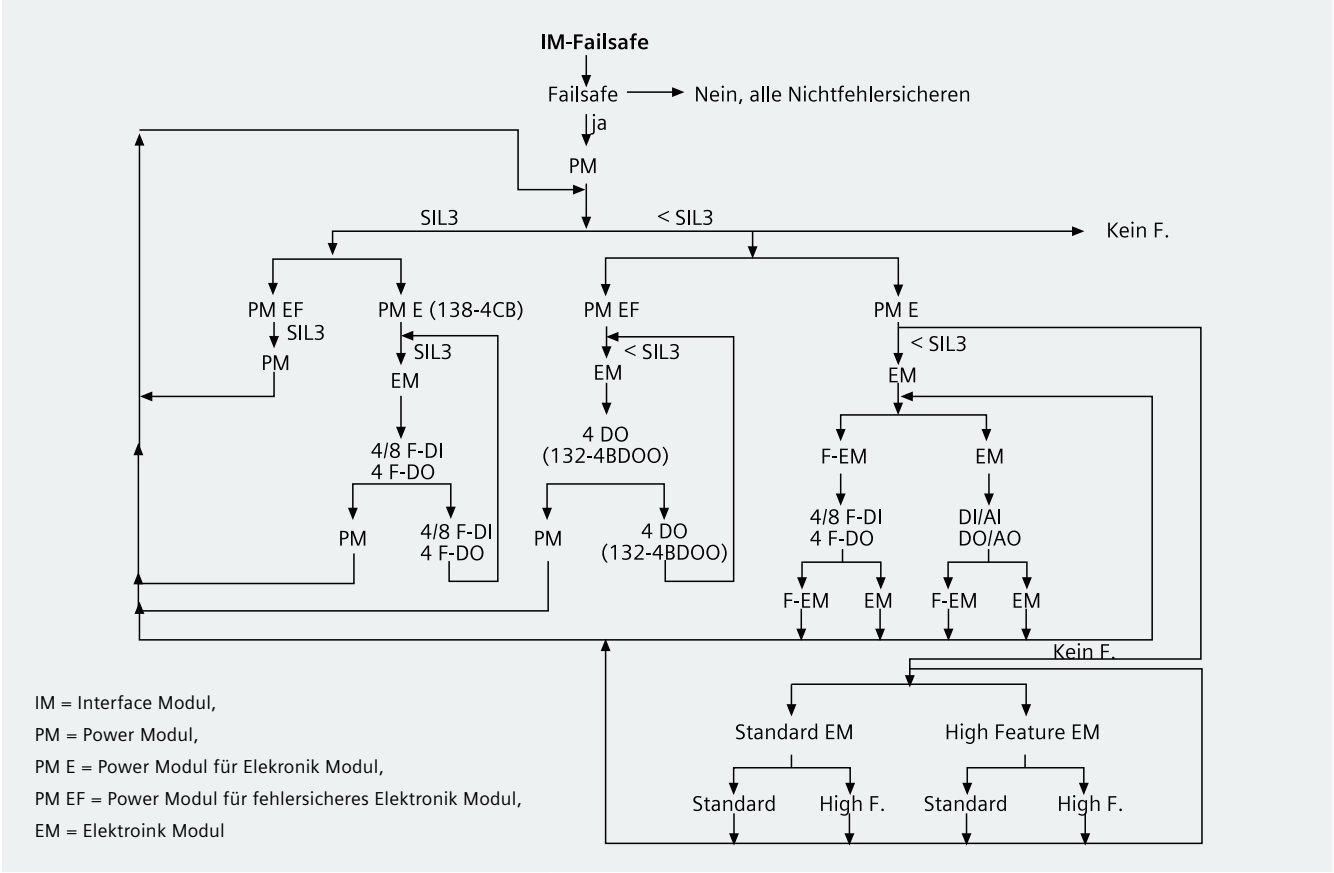


Bild 7/7
Struktur des ET 200S Konfigurators

In einer ET 200S oder ET 200M können fehlersichere und Standard-Baugruppen auch in Kombination betrieben werden. Je nach Systemaufbau kann hierbei bis SIL 3 bzw. Kat. 4 erreicht werden.

Konfiguratior für ET 200S

Um eine ET 200S Station richtig zu konfigurieren, ist seit April 2003 auf dem elektronischen CA01 Katalog ein ET 200S Konfigurator verfügbar, der nach folgender Spezifikation eine Hilfe gibt, um die Module zusammenzustellen. Betrachtet wird die Konfiguration von I/O Modulen und MS (Motorstartern) mit und ohne Sicherheitstechnik.

Ausgehend von der Kopfbaugruppe IM-Failsafe muss entschieden werden, welche Sicherheitskategorie die Lastkreise mit den Modulen erfüllen sollen. Danach kann mit dem Aufbau der Module begonnen werden. Im folgenden wird anhand von 2 Beispielen die Funktion des Konfigurators erklärt.

1. Standard Aufbau mit PM-E, F-DI und F-DO Modulen zur Erreichung von Kat. 4 bzw. SIL 3

Ein Lastkreis mit fehlersicheren F-DI und F-DO Baugruppen erfüllt die höchste Sicherheitskategorie Kat. 4 bzw. SIL 3. Die Einspeisung der Energie erfolgt über ein Standard Powermodul PM-E. Werden zusätzlich Standardmodule in einem Lastkreis mit F Modulen aufgebaut, kann max. die Sicherheitskategorie Kat. 3 bzw. SIL 2 erreicht werden.

2. Kostengünstiger Aufbau mit PM-E F und nachgeschalteten Standard 4-DO Modulen zur Erreichung von Kat. 3 bzw. SIL 2

Ein Lastkreis mit PM-E F Modulen und nachgeschalteten Standard 2-DO Modulen erfüllt maximal die Sicherheitskategorie Kat. 3 bzw. SIL 2. Über einen integrierten Relaisausgang im PM-E F kann sogar nach SIL 3 abgeschaltet werden.

7.8 Beispiele

Typische Konfigurationsbeispiele

Im Folgenden finden sich zwei Konfigurationsbeispiele für SIMATIC Safety Integrated – eines mit Schwerpunkt Fertigungsautomatisierung und eines aus dem Umfeld der Prozessautomatisierung

Sowohl die Standard-Kommunikation als auch die sicherheitsgerichtete Kommunikation erfolgt auf dem gleichen Standard-PROFIBUS-Kabel mit dem speziell für Sicherheitstechnik herstellerunabhängig entwickelten Busprofil PROFIsafe.

Fertigungsautomatisierung

Controller

- Fehlersichere CPUs für ET 200S, S7-300, S7-400

Peripherie

- SIMATIC ET 200M mit großer Anzahl von E/A-Baugruppen, feinmodulare SIMATIC ET 200S (IP20) und SIMATIC ET 200eco (IP65/67)
- NAMUR-Baugruppe der SIMATIC ET 200S für den Ex-Bereich
- Je nach Anforderung um Standard- und fehlersichere Baugruppen erweiterbar
- Fehlersichere Baugruppen: intern komplett redundant und diversitär aufgebaut
- Umfassende Diagnosefunktion zur Erkennung interner und externer Fehler
- Sicherheitsfunktionen sind in den fehlersicheren Signalbaugruppen enthalten
- Laserscanner LS4 mit PROFIsafe-Direktanbindung
- Motorstarter für ET 200S
- Frequenzumrichter für ET 200S

Kommunikation

- Standard-PROFIBUS DP mit PROFIsafe-Profil

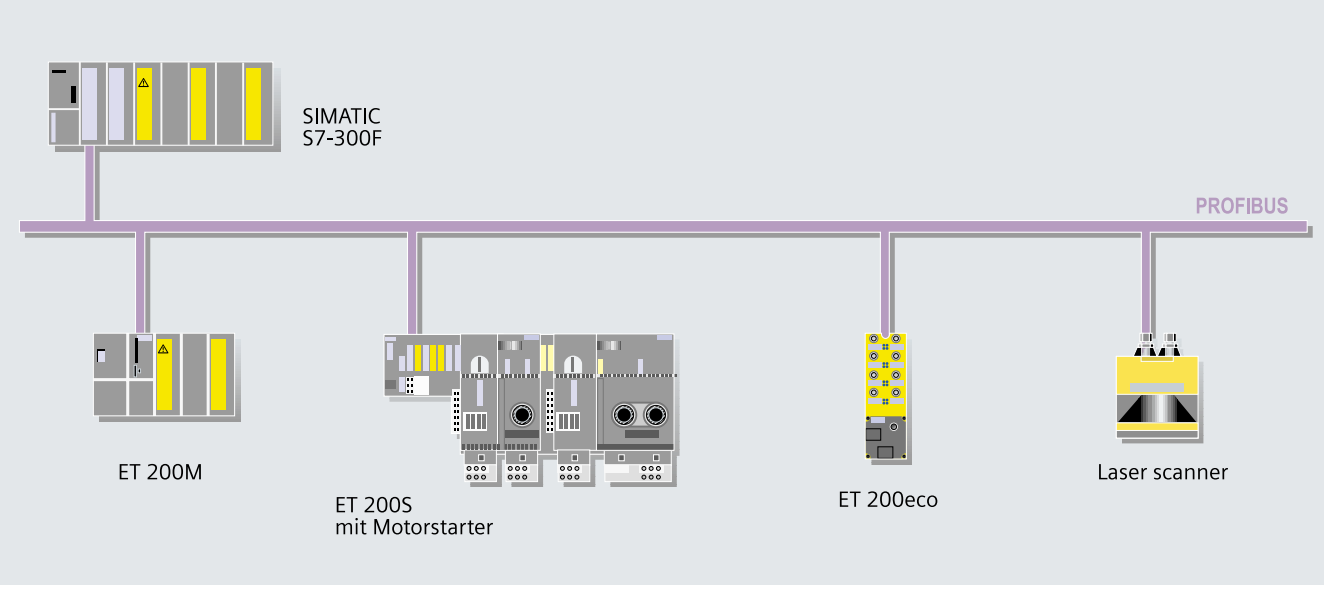


Bild 7/8
Konfigurationsbeispiel Fertigungsautomatisierung mit einfachen Aufbau

Prozessautomatisierung

Controller

- Sichere und fehlertolerante SIMATIC S7-400FH – projektierbar wie Standard-S7-400.
- Höchste Sicherheitsstufe SIL 3 mit nur einem Controller erfüllbar.
- Standard- und Sicherheitsfunktionen wahlweise in einem Controller vereint oder getrennt aufbaubar.
- Hohe Verfügbarkeit durch redundanten Aufbau eines zweiten Controllers möglich.
- Komplett integrierbar in SIMATIC PCS 7, aber auch anschließbar an jedes beliebige DCS (Distributed Control System).

Peripherie

- SIMATIC ET 200M mit großer Anzahl von E/A-Baugruppen und feinmodulare SIMATIC ET 200S.
- NAMUR-Baugruppe der SIMATIC ET 200M für den Ex-Bereich.
- Je nach Anforderung um Standard- und fehlersichere Baugruppen erweiterbar.
- Fehlersichere Baugruppen: intern komplett redundant und diversitär aufgebaut.
- Umfassende Diagnosefunktionen zur Erkennung interner und externer Fehler.
- Sicherheitsfunktionen in den fehlersicheren Signalbaugruppen enthalten.

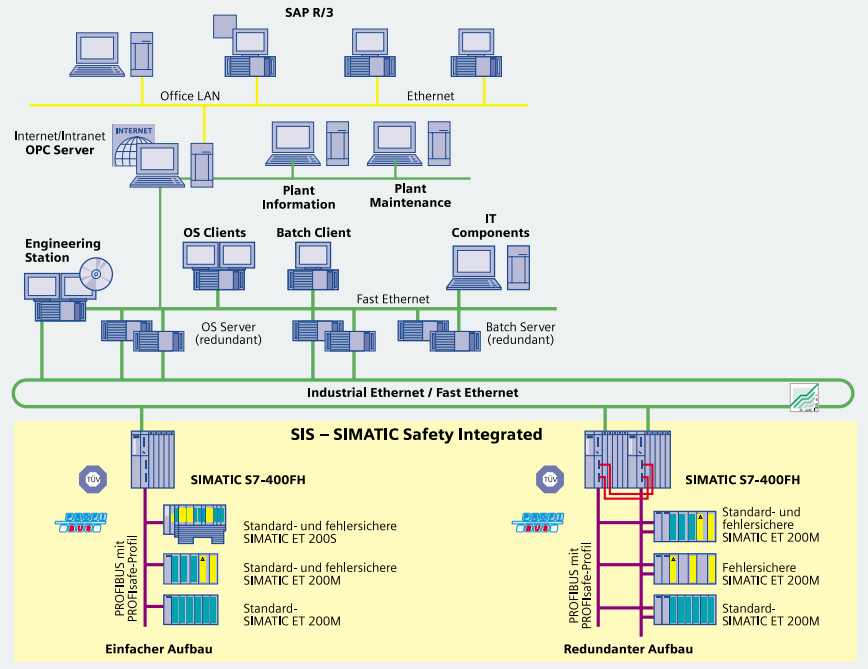


Bild 7/9
Konfigurationsbeispiel Prozessautomatisierung

Kommunikation

- Standard-PROFIBUS DP mit PROFIsafe-Profil

Mit SIMATIC Safety Integrated bieten wir eine erstklassige Safety Instrumentated System Lösung (SIS) auf Basis innovativer und bewährter Produkte, Systeme und Standards. SIMATIC Safety Integrated können Sie komfortabel an jedes beliebige Leitsystem anschließen - in SIMATIC PCS 7 ist es bereits heute integriert.

Programmieroberfläche Fertigungsautomatisierung

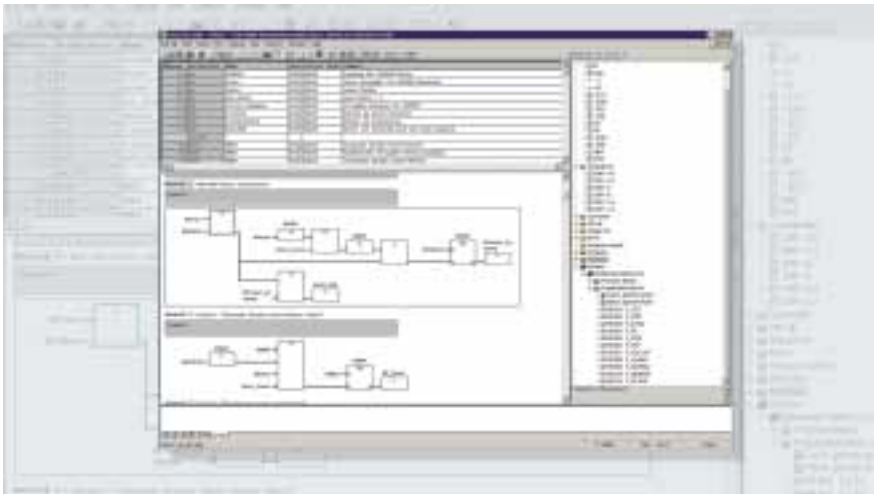


Bild 7/10
Programmieren mit dem Funktionsplan

Programmierbeispiel Fertigungsautomatisierung

Das Beispiel Not-Halt in Bild 7/11 zeigt, wie Stop-Funktionen sofort (Kategorie 0) oder verzögert (Kategorie 1) realisiert werden können. Die Quittier-Taste wird als Start-Eingang verwendet.

Durch die dezentrale Fehlerauswertung bei den ET 200-Modulen wird der Programmieraufwand minimiert. Z.B. wird die Diskrepanzzeit durch die HW-Konfigurierung projektiert, im Modul ausgewertet und im SPS-Programm erscheint nur noch ein Signal. Dieses vom System ermittelte Signal ist somit sehr einfach im Programm zu verarbeiten, und umständliche Berechnungen entfallen.

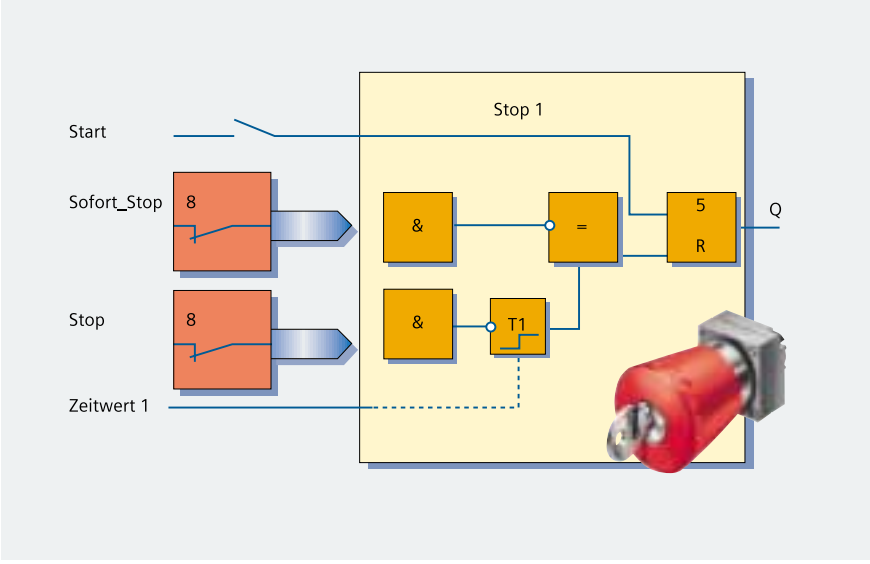


Bild 7/11
Programmierbeispiel „Not-Halt"

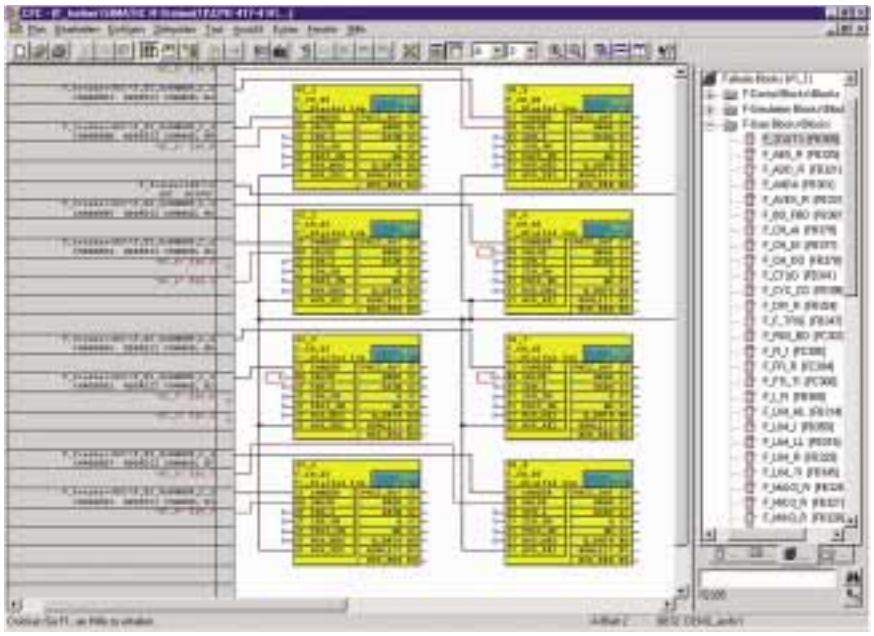


Bild 7/12

Grafische Projektierung der S7-400FH mit dem Engineering Tool Continuous Function Chart (CFC)

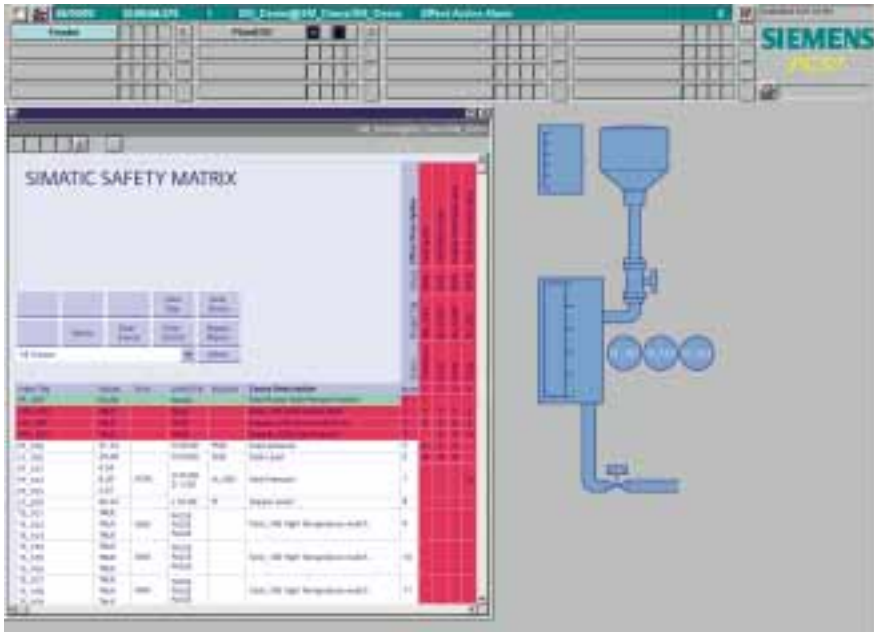


Bild 7/13

Die Safety Matrix erzeugt aus einer cause & effect-Tabelle ein ablauffähiges Programm

Projektierungsoberfläche Prozessautomatisierung

CFC erlaubt die grafische Projektierung von sicherheitsgerichteten Funktionen. Dabei können zertifizierte Funktions-Bausteine direkt aus der Bibliothek verwendet werden.

Alternativ kann das Projektierungstool SIMATIC Safety Matrix eingesetzt werden, das auf der einen Seite automatisch Cause & Effect Verknüpfungen in CFC übersetzt und auf der anderen Seite problemlos integrierbar und visualisierbar in PCS 7 ist.

7.9 Technische Daten

CPU	IM 151-7 F-CPU	CPU 315F-2 DP	CPU 317F-2 DP	CPU 416F-2
Aufbautechnik	ET 200S	S7-300 mit zentraler und/oder dezentraler fehlersicherer Peripherie		S7-400 mit dezentraler fehlersicherer Peripherie
Anwendungsbereich	• Dezentrale Anwendungen im unteren Leistungsbereich • Standalone-Systeme	• Mittlerer Leistungsbereich	• Mittlerer bis oberer Leistungsbereich	• Oberster Leistungsbereich
Arbeitsspeicher	48 kB	192 kB	512 kB	1,4 MB Daten 1,4 MB Code
Ladespeicher (steckbar)	64 kB - 8 MB	64 kB - 8 MB	64 kB - 8 MB	256 kB integriert 64 kB - 64 MB
Merker	2 kBit	16 kBit	64 kBit	128 kBit
FB/FC/DB	512/512/511	2048/2048/1023	2048/2048/2047	2048/2048/4095
Fehlersichere E/A	bis 28	bis 320	> 500	> 1000
Peripherieadressbereich E/A	244 B/244 B	2 kB/2 kB	8 kB/8 kB	16 kB/16 kB
Prozessabbild E/A	128 B/128 B	384 B/384 B	1 kB/1 kB	16 kB/16 kB
Schnittstellen	MPI/DP	MPI und DP	MPI/DP und DP	MPI/DP und DP
PFD*)	1,59E-05	2,38E-05	4,76E-05	4,76E-05
PFH*)	3,62E-10	5,42E-10	1,09E-09	1,09E-09
Maße	60 x 120 x 75	40 x 125 x 130	80 x 125 x 130	25 x 290 x 219
Bestell-Nr.-Rumpf	6ES7 151-7FA..	6ES7 315-6FF..	6ES7 317-6FF..	6ES7 416-2FK..

*) *PFD = Average probability of failure on demand*

*) *PFH = Probability of a dangerous failure per hour*

Optionspaket	S7 Distributed Safety	Brenner
Bibliothek	Zertifizierte Bausteine, z.B. Not-Aus, Zweihand-steuerung, Muting, Tür-überwachung	Zertifizierte Brenner-Bausteine
Voraussetzung	STEP 7	S7 Distributed Safety
Engineering-Paket	1 Lizenz pro Engineering-Platz erforderlich	
Runtime-Paket		1 Lizenz pro CPU erforderlich
Bestell-Nr.-Rumpf	6ES7 833-1FC..	9AL3 100-1AD..

CPUs Prozessautomatisierung

CPU	CPU 414-4H	CPU 417-4H
Arbeitsspeicher (integriert)	768 kB Daten 768 kB Code	10 MB Daten 10 MB Code
Ladespeicher (integriert, RAM)	256 kB	
Ladespeicher (erweiterbar, RAM/FEPROM)	Bis 64 MB	
Merker	64 kBit	
FB/FC/DB	2048/2048/4095	6144/6144/8192
Peripherieadress-bereich E/A	8 kB/8 kB	16 kB/16 kB
Prozessabbild E/A	8 kB/8 kB	16 kB/16 kB
Schnittstellen	MPI/DP und DP	
PFD*)	1,24 E-04	noch nicht verfügbar
PFH*)	1,42 E-09	noch nicht verfügbar
Maße	25 x 290 x 219	
Bestell-Nr.-Rumpf	6ES7414-4H...	6ES7417-4H...

Optionspaket	S7 F Systems	Brenner
Bibliothek	ca. 50 zertifizierte Grundfunktionsbausteine	Zertifizierte Brenner-Bausteine
Voraussetzungen	• STEP 7 • CFC • S7-SCL	• S7 F-Systems
Engineering-Paket	1 Lizenz pro Engineering-Platz erforderlich	
Runtime-Paket	1 Lizenz pro CPU erforderlich	
Bestell-Nr.-Rumpf	6ES7 833-1CC..	9AL3 100-1AA..

Gemeinsame Peripherie

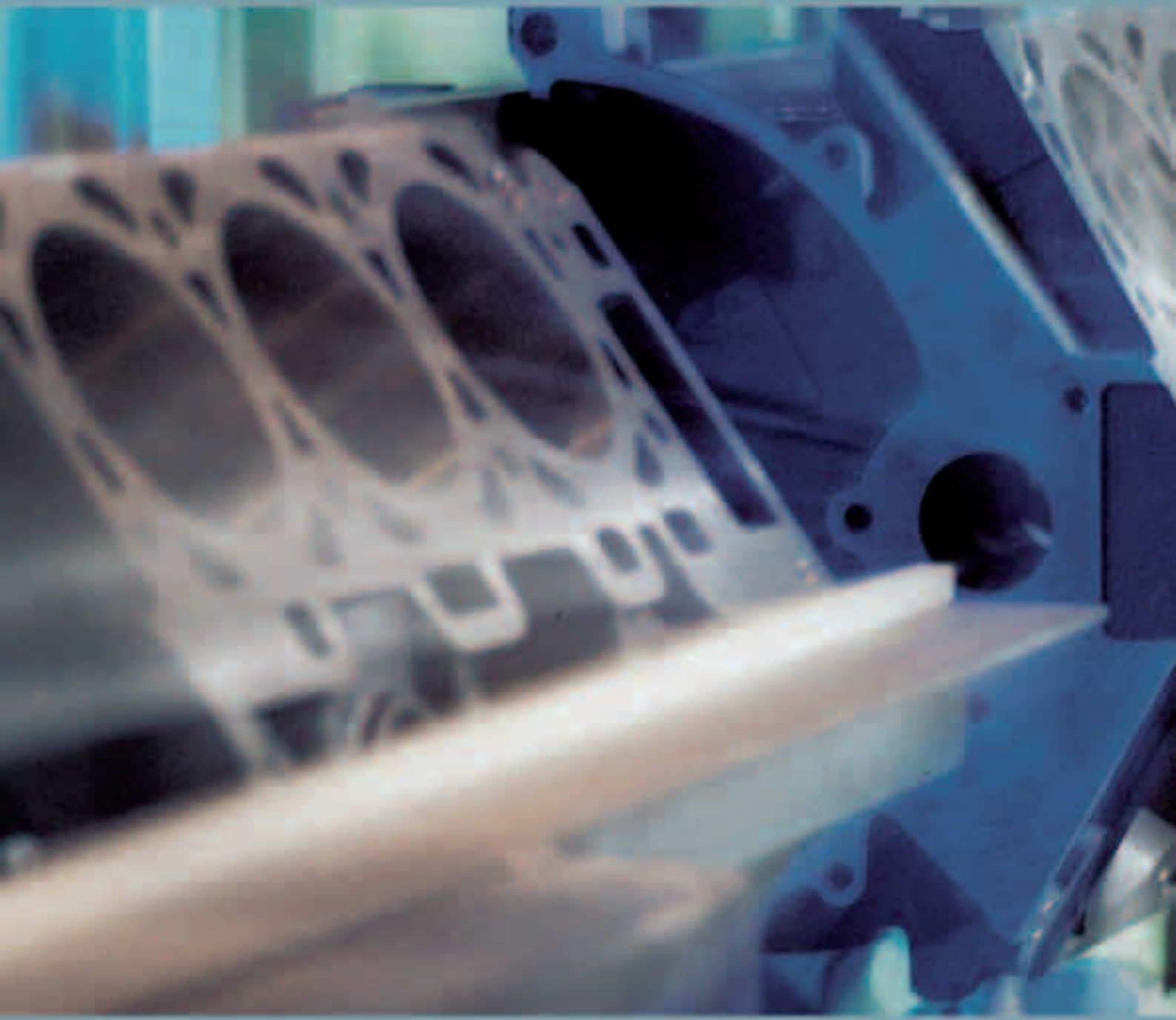
Fehlersichere S7-300 Signal-baugruppen	Digitaleingabe SM 326 F DI 24 x DC 24 V	Digitaleingabe SM 326 F 8 x (NAMUR)	Digitalausgabe SM 326 F DO 10 x DC 24 V/2A	Digitalausgabe SM 326 F DO 8 x DC 24 V/2A	Analogeingabebau-gruppe SM 336 F
Anzahl der Eingänge bzw. Ausgänge	24 (1-kanalig bei SIL 2-Sensoren) 12 (2-kanalig bei SIL 3-Sensoren)	8 (1-kanalig) 4 (2-kanalig)	10	8	6 (2-kanalig bei SIL 3-Sensoren) 13 Bit
Ein- bzw. Ausgangsspannung	DC 24 V	NAMUR	DC 24 V	DC 24 V P-M-schaltend	--
Alarme	Diagnosealarm	Diagnosealarm	Diagnosealarm	Diagnosealarm	--
Eingangsstrom/ Ausgangsstrom	--	--	2 A pro Kanal bei Signal „1“	2 A pro Kanal bei Signal „1“	4-20 mA
PFD*)	SIL2: 1,55E-06 SIL3: 4,99E-08	SIL2: 2,74E-06 SIL3: 4,83E-08	6,97E-06	noch nicht verfügbar	4,96E-08
PFH*)	SIL2: 1,77E-11 SIL3: 5,70E-13	SIL2: 3,13E-11 SIL3: 5,51E-13	7,96E-11	noch nicht verfügbar	5,66E-13
Bestell-Nr.-Rumpf	6ES7 326-1BK..-....	6ES7 326-1RF..-....	6ES7 326-2BF..-....	6ES7 326-2BF4.-...	6ES7 336-1HE..-....

Fehlersichere ET 200S-Module	Digitaleingabe 4/8 F-DI DC 24 V	Digitalausgabe 4 F-DO DC 24 V	Power Modul PM-PM-D F DC 24 V	Power Modul PM-PM-E F pp DC 24 V	Power Modul PM-PM-E F pm DC 24 V
Anzahl der Eingänge/Ausgänge	4 (2-kanalig bei SIL 3-Sensoren) 8 (1-kanalig bei SIL 2-Sensoren)	4 bei 24 V/2 A	6 Abschaltgruppen je 3A (Summenstrom 5 A)	2 Relais (Summenstrom 10 A)	bis zu 2 SIL 3-Ausgänge für 24 V/2 A, 2 Relais (Summenstrom 10 A)
Ein- bzw. Ausgangsspannung	DC 24 V	DC 24 V	DC 24 V	DC 24 V	DC 24 V
PFD*)	SIL2: << 1,00E-03 SIL3: << 1,00E-05	<< 1,00E-05	noch nicht verfügbar	noch nicht verfügbar	SIL2: << 1,00E-05 SIL3: << 1,00E-05
PFH*)	SIL2: << 1,00E-08 SIL3: << 1,00E-10	<< 1,00E-10	noch nicht verfügbar	noch nicht verfügbar	SIL2: << 1,00E-10 SIL3: << 1,00E-10
Bestell-Nr.-Rumpf	6ES7 138-4FA..-....	6ES7 138-4FB..-....	3RK1903-3BA..-....	6ES7 138-4CF4.-....	6ES7 138-4CF..-....

Motorstarter Fail-safe	
Leistung bei 500 V	7,5 kW
Bemessungsbetriebsstrom IE	16 A
Kurzschlussausschaltvermögen	50 kA bei 400 V
Codierung	Zuordenbar auf 1 von 6 Abschaltgruppen
Bestell-Nr.-Rumpf Motorstarter	3RK1301-0.B13-.AA2
Bestell-Nr.-Rumpf Terminalmodul	3RK1903-3A...
Fail-safe Contact Multiplier F-CM	
Kontakte	4 NO
Diagnose	Spannungsausfall, Gerätefehler
Schaltvermögen	1,5 A/24 V
Bestell-Nr.-Rumpf	3RK1 903-3CA..
Fail-safe Power Modul PM-D F X1 (Einspeiseklemmenmodul)	
Betrieb	Standalone mit externer Sicherheitstechnik
Doppelklemmen für Abschaltgruppen	6
Diagnose	Spannungsausfall
Bestell-Nr.-Rumpf	3RK1 903-3DA..

Frequenzumrichter Fail-safe	
Leistung	Bis 4,0 kW
Bestell-Nr.-Rumpf	6ES7 148-3FA..-....

Digitale Blockperipherie ET 200eco	
Anzahl der Eingänge	4 (2-kanalig bei SIL 3-Sensoren) 8 (1-kanalig bei SIL 3-Sensoren)
Eingangsspannung	DC 24 V
PFD*)	SIL2: << 1,00E-03 SIL3: << 1,00E-05
PFH*)	SIL2: << 1,00E-08 SIL3: << 1,00E-10
Bestell-Nr.-Rumpf	6ES7 148-3FA..-....



8.1 SINUMERIK Safety Integrated –
Das Sicherheitspaket für Bearbeitungsmaschinen

8.2 Safety Unit

8.3 Safety Integrated für Motion Control Systeme

Fehlersichere Motion Control Systeme

8

sinumerik

8 Fehlersichere Motion Control Systeme

8.1 SINUMERIK Safety Integrated – Das Sicherheitspaket für Bearbeitungsmaschinen

Antriebe und CNC-Steuerungen mit integrierter Sicherheit

Den Anspruch, den unsere Motion Control Systeme und drehzahlveränderbaren Antriebe für Werkzeug- und Produktionsmaschinen erfüllen, ist hoch: Sie integrieren alle Anforderungen von Produktion, Markt und Branche. Das trägt bei unseren Kunden dazu bei, die Qualität zu steigern und die Produktivität zu erhöhen. Zertifizierte Sicherheitsfunktionen sind integraler Bestandteil unserer Standardprodukte und leisten, neben einem hochwirksamen Schutz für Mensch und Maschine, ebenso einen Beitrag zur Steigerung der Produktivität beim Kunden.

Zum Schutz von Personen vor gefahrbringenden Bewegungen müssen an Maschinen Sicherheitsmaßnahmen vorgesehen werden. Diese dienen dazu, vor allem bei geöffneten Schutzeinrichtungen gefährliche Maschinenbewegungen zu verhindern. Zu diesen Funktionen zählen das Überwachen von Positionen, z.B. Endlagen, das Überwachen von Geschwindigkeiten und der Stillstand oder das Stillsetzen in Gefahrensituationen.

Zur technischen Umsetzung der Sicherheitsmaßnahmen wurden bisher überwiegend externe Einrichtungen verwendet. Dies sind Schütze, Schalter, Nocken und Überwachungsgeräte.

Bei Erkennen einer Gefahrensituation bewirken diese Einrichtungen im Allgemeinen eine kontaktbehaftete Schalthandlung im Leistungskreis, die zum Stillsetzen der Bewegungen führt, siehe Bild 8/1.

Bei der Integration von Sicherheitsfunktionen übernehmen Antriebssysteme und CNC-Steuerungen zusätzlich zu ihren Funktions- auch Sicherheitsaufgaben. Aufgrund der kurzen Datenwege von der Erfassung der sicherheitsrelevanten Information, z.B. Drehzahl oder Position, bis zur Auswertung sind sehr kurze Reaktionszeiten erreichbar.

Die Systeme mit integrierter Sicherheitstechnik reagieren im Allgemeinen sehr schnell auf die Überschreitung zulässiger Grenzwerte, z.B. Positions- oder Geschwindigkeitsgrenzwerte. Dies kann für das gewünschte Überwachungsergebnis von entscheidender Bedeutung sein. Die integrierte Sicherheitstechnik kann direkt auf die Leistungshalbleiter im Antriebsregelgerät zugreifen, ohne elektromechanische Schalteinrichtungen im Leistungskreis zu verwenden. Dies kommt einer verminderten Störanfälligkeit zugute. Schließlich verringert sich durch die Integration der Verdrahtungsaufwand.

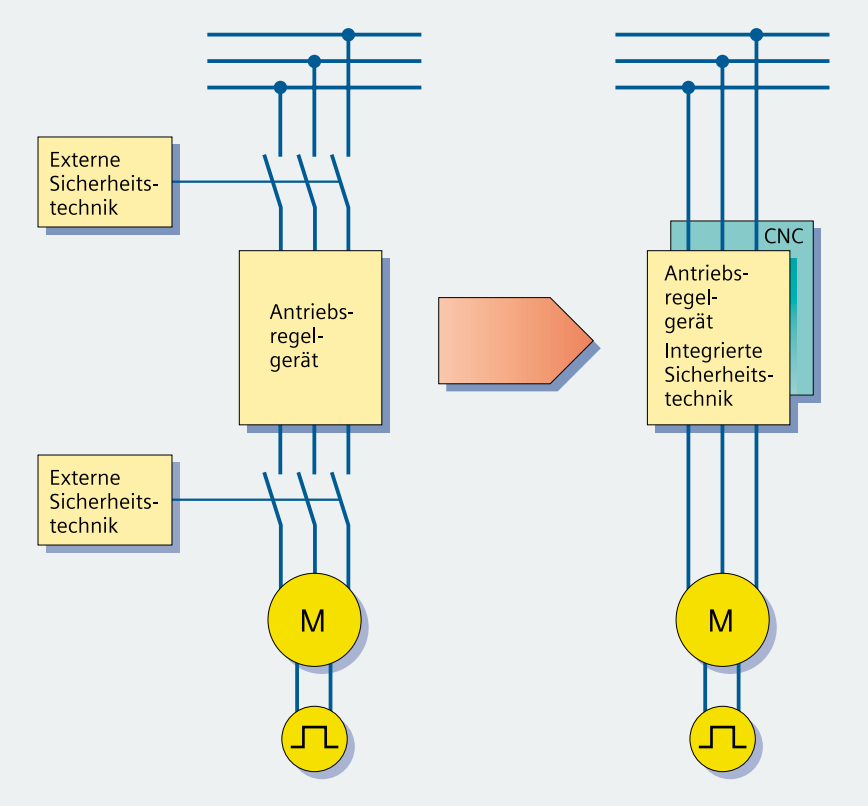


Bild 8/1
Externe Sicherheitstechnik, integrierte Sicherheitstechnik

Bild 8/2
Das Grundsystem SINUMERIK/SIMODRIVE

Kurzbeschreibung

Funktionsumfang

„SINUMERIK Safety Integrated" bietet baumustergeprüfte Sicherheitsfunktionen, mit denen sich ein hochwirksamer Personen- und Maschinenschutz praxisgerecht realisieren lässt. Alle Sicherheitsfunktionen erfüllen die Anforderungen der Kategorie 3 nach EN 954-1 und sind fester Bestandteil des Grundsystems. Es sind keine zusätzlichen Sensoren oder Auswertegeräte erforderlich.

Das bedeutet:

Weniger Installationsaufwand an der Maschine und einen „schlanken" Schaltschrank.

Zum Funktionsumfang gehören z.B.:

- Funktionen zur sicheren Überwachung von Geschwindigkeit, Stillstand und Position
- Funktionen zur sicheren logischen Verknüpfung von Signalen

Sensoren und Aktoren, wie beispielsweise Not-Halt-Taster, Lichtvorhänge, Ventile oder Bremsen, können direkt an eine 2-kanalige Peripherie oder an failsafe-Baugruppen angeschlossen werden. Die logische Verknüpfung und die Reaktionen erfolgen intern in sicherer Technik. Grundsätzlich führen alle sicherheitsrelevanten Fehler im System zu einem sicheren Stillsetzen der gefahrbringenden Bewegung oder zur schnellen, kontaktfreien Energietrennung zum Motor. Das Stillsetzen der Antriebe erfolgt stets optimal, angepasst an den Betriebszustand der Maschine. So kann z.B. im Einrichte-Betrieb bei geöffneter Schutztür schnellstmöglich (optimal für Personenschutz) und im Automatik-Betrieb mit geschlossener Schutztür bahnbezogen (optimal für Maschinenschutz) stillgesetzt werden.

Die Sicherheitsfunktionen stehen in allen Betriebsarten zur Verfügung und können über sicherheitsgerichtete Ein-/Ausgangssignale mit dem Prozess kommunizieren. Sie erfüllen die Anforderungen der Kategorie 3 (nach EN 954-1). Der gesamte Funktionsumfang wurde im Rahmen einer Baumusterprüfung vom BIA in St. Augustin zertifiziert.

Das bedeutet:

Hoher Personenschutz im Einrichte-Betrieb und zusätzlicher Schutz für Maschine, Werkzeug und Werkstück im Automatik-Betrieb.

Die Sicherheitsfunktionen bieten einen bisher nicht gekannten, intelligenten Systemdurchgriff direkt bis hin zu den elektrischen Antrieben und Messsystemen. Zuverlässige Funktion, schnelle Reaktion und breite Akzeptanz verleihen diesem zertifizierten Sicherheitssystem eine hohe Wirksamkeit.

Grundstruktur

Mit der vorhandenen Mehrprozessorstruktur wird eine 2-kanalige, diversitäre Systemstruktur gebildet. Die Sicherheitsfunktionen sind redundant in NC, Antrieb und interner PLC eingebunden. Die Prozessgrößen und sicherheitsrelevanten Systemdaten werden kreuzweise verglichen, siehe Bild 8/3.

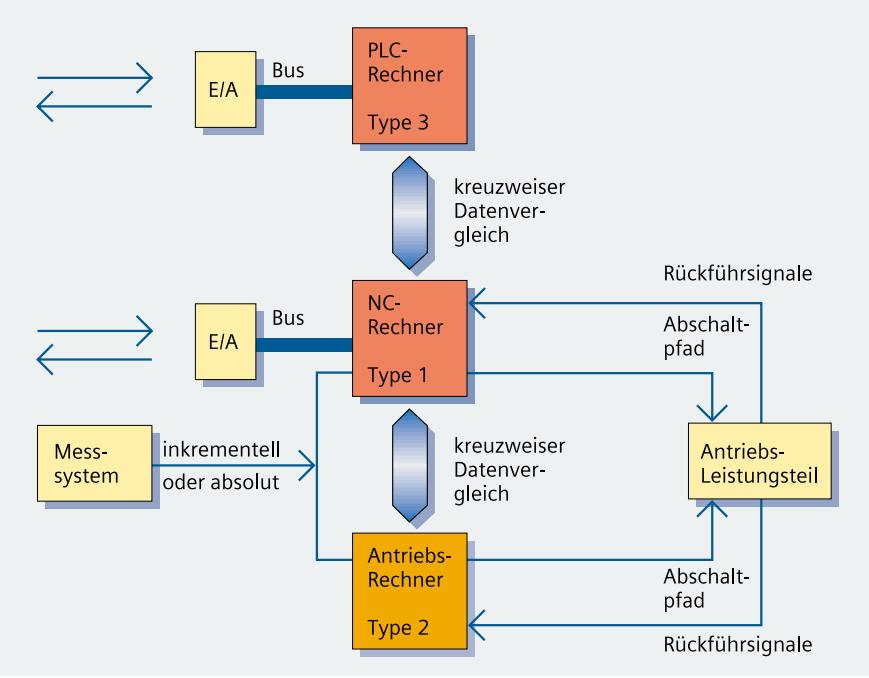


Bild 8/3
Vorhandene Rechner bilden eine zweikanalige, diversitäre Systemstruktur

Sicherheitsgerichtete Software- und Hardwarefunktionen werden durch eine automatisierte Zwangsdynamisierung in definierten Zeitabständen geprüft.

Eine Besonderheit dieses Sicherheitskonzeptes ist, dass schon mit nur einem Messsystem, dem Standard-Motormesssystem, die Kategorie 3 nach EN 954-1 realisierbar ist. Ein zweiter Messgeber ist nicht erforderlich, kann jedoch als zusätzliches, direktes Messsystem (z.B. Linearmaßstab) eingebunden werden.

Verfügbarkeitssteigerung durch integrierte Sicherheitstechnik

Durch Kombination der Sicherheitsfunktionen von SINUMERIK Safety Integrated lassen sich völlig neue Bedienkonzepte an Maschinen mit unterschiedlichsten Anforderungen realisieren. Eingriffe des Bedieners, z.B. im Magazin oder am Umrüstplatz (Einrichten), können parallel zur laufenden Produktion erfolgen.

Im Vordergrund steht dabei jedoch immer der optimale Schutz des Bedieners. Die durch den Prozess vorgegebene bestimmungsgemäße Verwendung der Maschine muss erhalten bleiben.

Von diesen neuen Möglichkeiten kann auch der Maschinenschutz (Maschine, Werkstück, Werkzeug, ...) in einem hohen Maße profitieren.

Durch die integrierte Sicherheitstechnik geht der Trend weg von rein hardware- und elektromechanisch geprägten Lösungen hin zu Software und Elektronik und ersetzt damit sukzessive verschleißbehaftete Technik.

Weiterhin ermöglicht integrierte Sicherheitstechnik einen bisher nicht gekannten, intelligenten Systemdurchgriff direkt bis hin zu den Sensoren und Aktoren. Es entstehen neue Diagnosemöglichkeiten, die im Besonderen eine präventive Fehleraufdeckung erlauben. Auch bei plötzlich auftretenden Fehlern während der Produktion kann durch eine schnelle Fehleraufdeckung und ein koordiniertes, sicheres Stillsetzen das Risiko eines Personen- oder Maschinenschadens erheblich reduziert werden.

Integrierte Sicherheitstechnik ermöglicht:

- Optimierte Prozessabläufe
- Parallele Abläufe von Teilprozessen
- Einfachere Maschineninfrastrukturen
- Praxisgerechte Maschinenbedienkonzepte.

Auswirkung auf die Verfügbarkeit:

- Reduziertes Fehlerpotenzial
- Längere Produktionszeiten
- Kürzere Stillstandszeiten.

Integrierte Sicherheitstechnik bietet, bei konsequenter Nutzung, ein großes Potenzial zur Steigerung der Verfügbarkeit.

Ausrüstungskomponenten

Im Geschäftsgebiet „Automatisierungs- und Antriebstechnik Motion Control Systeme“ entwickeln, fertigen und vertreiben wir numerische Steuerungen und Antriebssysteme unter den Produktnamen SINUMERIK und SIMODRIVE, die vor allem bei komplexen und hochdynamischen Bewegungsaufgaben sowie bei Positionieranwendungen mit besonderen Anforderungen an die Präzision eingesetzt werden.

CNC-Steuerung SINUMERIK 840D – Hightech kompakt

Die SINUMERIK 840D ist eine CNC-Steuerung für bis zu 31 Achsen. Mit ihrem Aufbaukonzept ist sie ein integraler Bestandteil des modularen Antriebssystems SIMODRIVE 611. Die Kommunikation mit den angereihten Antriebsmodulen ist somit auf kürzestem Wege möglich.

Aufbauend auf dem Systembaukasten SIMODRIVE 611 ist mit der SINUMERIK 840D ein Baustein konzipiert worden, der erhebliche technische Vorteile gegenüber vergleichbaren Einzellösungen bietet.

Highlights:

- Positionierung von bis zu 31 Achsen
- Präzision unter 1 µm
- Integrierte SIMATIC S7-300-CPU mit PROFIBUS-DP-Schnittstelle
- Nur 50 mm breit im SIMODRIVE 611digital-Aufbau
- Skalierbare Prozessorleistung
- Integrierte, zertifizierte Sicherheitsfunktionen

Bild 8/4
SINUMERIK 840D – NCU und NCU-Box

Frequenz-Umrichter SIMODRIVE 611 digital

SIMODRIVE 611digital ist ein flexibel projektierbares Umrichtersystem, das sowohl ökonomisch als auch ökologisch für die technischen Anforderungen von modernen Maschinen ausgerichtet ist. Mit SIMODRIVE 611digital bietet Siemens ein Umrichtersystem mit digitaler Regelung, das höchste Anforderungen an Dynamik, Drehzahlstellbereich und Rundlaufeigenschaften garantiert.

Durch den modularen Aufbau des Umrichtersystems lassen sich Antriebskonfigurationen mit nahezu beliebiger Achs- bzw. Hauptspindelanzahl verwirklichen. Die Achsmodule sind auf die Vorschubmotoren 1FT6, 1FK6, 1FK7 und 1FN sowie die Hauptspindelmotoren 1PH und die Synchron-Einbaumotoren 1FE ausgelegt.

Mit dem Umrichtersystem SIMODRIVE 611digital stehen Vorteile zur Verfügung wie:

- Erfüllung der EMV-Richtlinie und EMV-gerechte Netzeinspeisungen
- Geringe Netzbelastung durch Sinusstrombetrieb und Energierückspeisung
- Kompakter Aufbau durch Einsatz verlustarmer Leistungshalbleiter
- Hohe Funktionalität auf engstem Raum durch hochintegrierte Regelungselektronik

Die digitalen Regelungseinschübe des SIMODRIVE 611digital kommen in Verbindung mit den SIMODRIVE-Drehstrom-Servomotoren 1FT6/1FK6/1FK7 und Linearmotoren 1FN für Vorschubantriebe sowie den 1FE- und 1PH-Motoren für Hauptspindelantriebe zum Einsatz. Sie werten den im 1FT6/1FK6/1/FK7 oder 1PH-Motor eingebauten optischen Sinus-Cosinus-Geber aus. Damit können bis zu 4,2 Mio. Inkremente/Motorumdrehungen als Messkreisauflösung erreicht werden. Bei den Motoren 1FN ist ein linear inkrementelles oder absolut codiertes Messsystem mit EnDat-Schnittstelle zur Erfassung von Position, Drehzahl-Istwert und Pollage erforderlich. Die 1FE-Motoren benötigen für die Drehzahl- und Lageregelung einen Hohlwellengeber mit Sinus-Cosinus-Signalen. Bei den Regelungseinschüben mit direkter Lageerfassung kann zusätzlich ein direktes Messsystem angeschlossen werden. Die zertifizierten Sicherheitsfunktionen stehen für alle Geber-Varianten zur Verfügung.

Bild 8/5
Umrichtersystem SIMODRIVE 611digital

Bild 8/6
Digitaler Regelungseinschub

Mit dem modularen Umrichtersystem SIMODRIVE 611digital lassen sich unterschiedliche antriebstechnische Ausprägungen realisieren und in einem Antriebsverband beliebig kombinieren.

Servomotoren 1FK6/1FK7 und 1FT6

Sie sind die richtige Lösung, wenn höchste Dynamik und Präzision verlangt werden. Einfache und gute Regelbarkeit, kombiniert mit Eigenschaften wie Wartungsfreiheit und hoher Überlastbarkeit werden hier vom Anwender ganz besonders geschätzt.

Drehstrom-Servomotoren 1FK6/1FK7 und 1FT6 sind dauermagneterregte Synchronmotoren mit kompakten Abmessungen, die speziell für den Betrieb am Umrichtersystem SIMODRIVE 611digital entwickelt wurden. Die vollständig digitale Regelung und die neue integrierte Gebertechnik (Motormesssystem) erfüllen hohe Anforderungen an Dynamik, Drehzahlstellbereich, Rundlauf- und Positioniergenauigkeit.

Drehzahlgeregelte Spezial-Asynchronmotoren 1PH

Basierend auf der von Siemens entwickelten und patentierten Transvektorregelung ist es möglich, einen Asynchronmotor so einfach zu regeln wie einen Gleichstrommotor. Gegenüber diesem bietet ein durch SIMODRIVE 611digital geregelter Asynchronmotor Vorteile wie Wartungsfreiheit sowie Verfügbarkeit des Nenndrehmomentes bereits im Stillstand. Zur Drehzahlregelung und Positionierung sind die Motoren 1PH mit einem hochwertigen Gebersystem ausgerüstet.

Hauptspindelmotoren 1PM mit Hohlwelle

Die flüssigkeitsgekühlten 1PM4-Motoren und die luftgekühlten 1PM6-Motoren sind speziell für den direkten Anbau an mechanische Spindeln konzipiert. Die hohlgebohrte Welle ermöglicht die Zuführung für Kühlschmiermittel für innengekühlte Werkzeuge. Die Motoren verfügen über ein eingebautes Hohlwellenmesssystem zur Erfassung der Motordrehzahl und indirekten Lage.

Linearmotoren 1FN

Die Drehstrom-Linearmotoren 1FN bilden zusammen mit dem SIMODRIVE 611digital ein speziell auf die Belange der Werkzeugmaschine abgestimmtes lineares Antriebssystem. Die Motoren bestehen aus einem Primärteil und einem Sekundärteil mit Seltenerdmagneten. Bei Verwendung geeigneter Messsysteme können die Motoren im Nanometerbereich positioniert werden. Besonders herausragend aber sind die mit den Motoren erreichbaren hohen Verfahrgeschwindigkeiten und die extreme Dynamik.

Synchron-Einbaumotoren 1FE

Einbaumotoren 1FE sind wassergekühlte Synchronmotoren, die als Komponenten geliefert und vor allem als Hauptspindelantrieb eingesetzt werden. Diese Motoren kommen, gemeinsam mit dem Antriebsmodul SIMODRIVE 611digital, vor allem dort zum Einsatz, wo höchste Anforderungen an Bearbeitungsgüte, Genauigkeit, Laufruhe sowie kürzeste Hochlaufzeiten gestellt werden.

Bild 8/7
Servomotoren 1FT6

Bild 8/8
Asynchron-Einbaumotor 1PH

Bild 8/11
Asynchronmotor 1PH7

Bild 8/9
Linearmotor 1FN3

Bild /10
Synchron-Einbaumotor 1FE

Bild 8/12
Systemkomponenten und Verbindungstechnik

Zubehör

Die Siemens-Automatisierungssysteme SINUMERIK und SIMODRIVE sind für alle Bearbeitungsmaschinen ausgelegt. Optimal auf den Anwendungsbereich abgestimmt, bietet Siemens zu diesen Systemen mit der Leitungsfamilie MOTION-CONNECT die zugehörigen konfektionierten Leitungen, Meterware und Stecker.

Kundennutzen mit von Siemens konfektionierten Leitungen:

- Systemfunktionalität und -verträglichkeit sind gewährleistet
- EG-Richtlinien EMV sind erfüllt
- VDE-gerechte Isolation
- DESINA-konform
- Keine Montageprobleme
- Keine Spezialwerkzeuge erforderlich
- Mit MOTION-CONNECT 800, 700, 500 eine zugeschnittene Lösung für jeden Anwendungsfall
- Gewährleistung für die einwandfreie Funktion des Gesamtsystems

Optimal abgestimmt sind auch die ergänzenden Systemkomponenten wie Geber, Handräder, Bedien- und Programmierhandgeräte.

Messsysteme SIMODRIVE Sensor zur Erfassung von Wegstrecken, Drehwinkeln und Drehzahlen bietet Siemens in der Ausführung als Inkrementalgeber und Absolutwertgeber an. Bei den Inkrementalgebern sind die Interfaces auf die jeweilige Steuerung abgestimmt. Absolutwertgeber sind in den Ausführungen mit SSI, EnDat und PROFIBUS-DP verfügbar. Die Parametrierbarkeit der Geber ermöglicht eine komfortable und rasche Inbetriebsetzung. Durch systemgetestete Komponenten wird eine hohe Maschinenverfügbarkeit erreicht.

Das Originalzubehör von Siemens ist ein wesentlicher Bestandteil bei Applikationen mit SINUMERIK Safety Integrated.

Systemvoraussetzungen

Bestelldaten siehe Katalog NC 60 und ST76

SIMODRIVE 611digital

- Safety Integrated ist mit den digitalen Antrieben verfügbar
- Es lässt sich die High-Performance- und die High-Standard-Regelung des 611digital einsetzen
- Die Regelungsbaugruppen müssen immer mit DMS-Messkreis bestellt werden
- Es muss immer mindestens ein Messsystem verfügbar sein

SINUMERIK

Mit SINUMERIK ist Safety Integrated für die Typen 840C und 840D, in Verbindung mit SIMODRIVE 611digital, verfügbar. Dabei können alle CPU-Varianten eingesetzt werden.

- Ein-/Ausgänge für sicherheitsgerichtete Signale.
  1. NC-Peripherie und PLC-Peripherie bilden eine 2-kanalige E/A-Struktur
  oder
  2. Anbindung von Failsafe-Baugruppen über den PROFIBUS mit dem erweiterten PROFIsafe-Protokoll (nicht mit SINUMERIK 840C)
  oder
  3. NCU-Onboard I/Os und PLC-Peripherie bilden eine 2-kanalige E/A-Struktur (nicht mit SINUMERIK 840C)
- SINUMERIK Safety Integrated ist eine Softwareoption und setzt sich aus einer Basis- und den Achsoptionen zusammen.
- Für die SI-Funktionen werden Systemressourcen von den beteiligten CPUs (NC, PLC, Antrieb) benötigt, die abhängig vom Umfang der genutzten Funktionen und der Anzahl der Antriebe sind. In Grenzfällen kann der Einsatz einer höherwertigen NC-CPU erforderlich werden.

Geber und Messkreis

- Grundsätzlich lässt sich jedes Messsystem einsetzen, das die Messkreisspezifikation des SIMODRIVE 611D erfüllt.
- 1-Geber-Konzept: Es ist mindestens ein Messsystem erforderlich, das in der Regel mit dem indirekten Motormesssystem (IMS) als Inkrementalgeber oder Absolutgeber abgedeckt wird.
- 2-Geber-Konzept: Ein zweites Messsystem ist nicht erforderlich, es kann jedoch als direktes Messsystem (DMS) eingebunden werden.
- Die Messkreiskabel müssen der Spezifikation des SIMODRIVE 611 digital entsprechen, z.B. paarweise abgeschirmt sein.

SIMATIC

- Es lassen sich Standard-Komponenten der SIMATIC einsetzen.
- Ein-/Ausgänge für sicherheitsgerichtete Signale.
  1. NC-Peripherie und PLC-Peripherie bilden eine 2-kanalige E/A-Struktur
  oder
  2. Anbindung von failsafe-Baugruppen über den PROFIBUS mit dem herstellerunabhängigen PROFIsafe-Profil

HMI

- Nicht in das Sicherheitskonzept eingebunden sind die Bedien- und Anzeigegeräte (OPs). Sie dienen lediglich zur Anzeige von sicherheitsrelevanten Daten für Diagnose und Inbetriebsetzung.

Sicheres Stillsetzen

Sicheres Stillsetzen ist keine eigenständige Funktion, sondern beschreibt einen Vorgang, der mit Hilfe der-„SINUMERIK Safety Integrated"- Funktionen realisiert werden kann. Sicheres Stillsetzen führt die Antriebe beim Ansprechen einer Überwachung oder eines Sensors (z.B. Lichtvorhang) sicher aus der Bewegung in den Stillstand.

Grundsätzlich führen alle sicherheitsrelevanten Fehler im System oder das Ansprechen eines entsprechenden Sensors zu einem koordinierten, sicheren Stillsetzen der gefahrbringenden Bewegung. Je nach Projektierung kann auch eine schnelle Abtrennung der Energiezufuhr zum Motor erfolgen. Diese im speziellen Fall notwendige Energietrennung (Antriebe sind drehmomentfrei) zwischen Umrichter und Motor erfolgt kontaktfrei und kann mit einer sehr kurzen Ansprechzeit achsspezifisch ausgelöst werden. Eine Zwischenkreisentladung im Antrieb ist daher nicht mehr erforderlich. Das Stillsetzen der Antriebe erfolgt stets optimal, angepasst an den Betriebszustand der Maschine.

Das Aktivieren von externen Bremsmechanismen ergänzt die integrierten Funktionen und führt beim sicheren Stillsetzen zu einem möglichst kurzen Bremsweg. Externe Bremsmechanismen können z.B. sein:

- Externe mechanische Bremse, Halte- bzw. Betriebsbremse
- Externe elektrische Bremse wie z.B. Ankerkurzschlussbremse.

Ein Netzschütz ist prinzipiell nicht mehr erforderlich, wenn zur galvanischen Potenzialtrennung ein Hauptschalter an der Maschine vorhanden ist.

Stopreaktionen

Durch die 2-kanalige Überwachungsstruktur mit ihrem permanenten, kreuzweisen Datenvergleich ist eine hohe Fehlersicherheit gegeben. Bei auftretenden Differenzen zwischen den beiden Überwachungskanälen werden Alarme und Stopreaktionen automatisch ausgelöst. Die Stopreaktionen sollen die Antriebe, den jeweiligen Erfordernissen an der Maschine entsprechend geführt, sicher stillsetzen. Es wird zwischen den Stopvarianten STOP A, B, C, D, E, F und dem Teststop unterschieden. Die Art der Stopreaktion kann bei einem auftretenden Fehler vom System fest vorgegeben sein oder vom Maschinenhersteller projektiert werden. Bei der Überschreitung der über Maschinendaten festgelegten Grenzwerte von Funktionen können die Stopreaktionen vom Maschinenhersteller projektiert werden. Die Stops A, C und D können auch ereignisbezogen von extern über sicherheitsgerichtete Eingänge (SGE) angewählt werden. Die Wirkungsweise der Stopvarianten sind:

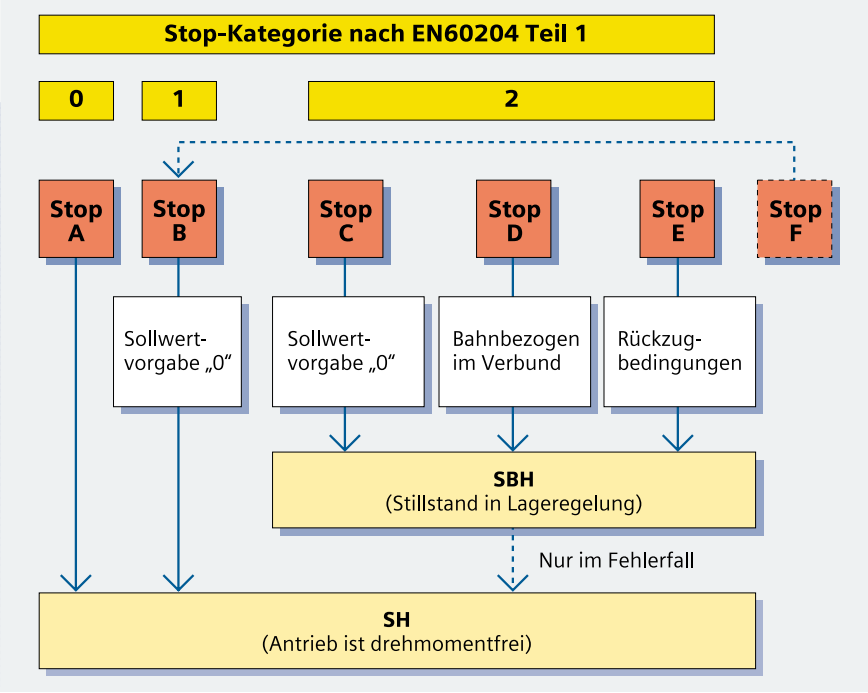


Bild 8/13
Stop-Varianten zum differenzierten Stillsetzen

- **Stop A**

Mit dem Stop A (entspricht Stop Kat. 0 nach EN 60204, ohne galvanische Trennung) wird der Antrieb über die Funktion „Sicherer Halt" direkt drehmomentfrei geschaltet. Ein im Stillstand befindlicher Antrieb kann nicht mehr ungewollt anlaufen. Ein Antrieb, der noch in Bewegung ist, trudelt aus. Dies kann verhindert werden durch den Einsatz von externen Bremsmechanismen wie Ankerkurzschluss, Halte- bzw. Betriebsbremse. Der achsspezifische Alarm zieht einen BAG-Stop (Betriebsartengruppe) nach sich, d.h. durch die Reaktion in einer Achse werden alle in einer BAG vorhandenen Achsen und Spindeln stillgesetzt. Am Ende von Stop A ist der „sichere Halt" (SH) wirksam.

- **Stop B**

Der Antrieb wird drehzahlgeregelt an der Stromgrenze abgebremst und in den „sicheren Halt" (SH) überführt (entspricht Stop Kat. 1 nach EN 60204, ohne galvanische Trennung).

- **Stop C**

Der Antrieb wird drehzahlgeregelt an der Stromgrenze abgebremst und in den „sicheren Betriebshalt" (SBH) überführt.

- **Stop D**

Der Antrieb wird im Verbund, inklusive Simultanachsen, bahnbezogen abgebremst und in den „sicheren Betriebshalt" (SBH) überführt.

- **Stop E**

Der Antrieb wird im Verbund, inklusive der Rückzugsbewegungen, bahnbezogen abgebremst und in den „sicheren Betriebshalt" (SBH) überführt.

- **Stop F**

Die Stop-F-Reaktion ist fest dem kreuzweisen Datenvergleich KDV zugeordnet. Es werden damit Fehler auf der Antriebs- und Steuerungsseite aufgedeckt. Es wird, je nach Projektierung, eine Stop-B- oder A-Reaktion ausgelöst. Am Ende ist der „sichere Halt" (SH) wirksam.

Bei der Projektierung der Stopreaktionen ist vorrangig der Personenschutz zu betrachten. Im Automatikbetrieb kann bei geschlossener Schutztür die optimale Stopreaktion für den Maschinenschutz projektiert werden. Angestrebt werden muss immer ein der Situation angemessenes bestmögliches Stillsetzen.

Beispiel 1: Schleifmaschine bei offener Schutztür (Einrichtbetrieb):

- Vorschubantriebe mit Stop C:
  Die Antriebe werden achsspezifisch, schnellstmöglich an der Stromgrenze gebremst und anschließend in den „sicheren Betriebshalt" überführt. Sie bleiben damit in Lageregelung.

- Schleifscheibenspindel mit externem Stop A:
  Der Antrieb wird in dieser Betriebsart generell über den externen Stop A mit „sicherem Halt" drehmomentfrei gehalten.

Beispiel 2: Schleifmaschine im Automatikbetrieb:

- Vorschubantriebe mit Stop E:
  Die Antriebe führen im Verbund eine Rückzugsbewegung aus (freischneiden/freifahren) und werden auf der Kontur über eine Rampe gebremst und anschließend in den „sicheren Betriebshalt" überführt. Sie bleiben damit in Lageregelung.

- Schleifscheibenspindel mit Stop D:
  Der Antrieb wird über eine Rampe abgebremst und damit von der Momentenbelastung her unterhalb der Berstgrenze gehalten. Er wird in den „sicheren Betriebshalt" überführt und in Lageregelung gehalten.

Sicherer Halt – SH

Der „sichere Halt" dient im Fehlerfall oder in Verbindung mit einer Maschinenfunktion zum sicheren Abtrennen der Energiezufuhr zum Motor. Dies erfolgt achsspezifisch und kontaktfrei. Die Basis für die Funktion „Sicherer Halt" ist die in den Antriebsmodulen des SIMODRIVE 611D integrierte sichere Impulslöschung.

Der Maschinenhersteller muss Maßnahmen gegen ungewollte Bewegungen nach dem Abtrennen der Energiezufuhr vom Motor treffen (z.B. gegen das Durchsacken vertikaler Achsen).

Funktionsmerkmale
- Es ist kein ungewollter Anlauf des Motors möglich.
- Die Energiezufuhr zum Motor ist sicher unterbrochen.
- Es erfolgt keine galvanische Trennung des Motors vom Antriebsmodul bzw. Zwischenkreis des Umrichters.

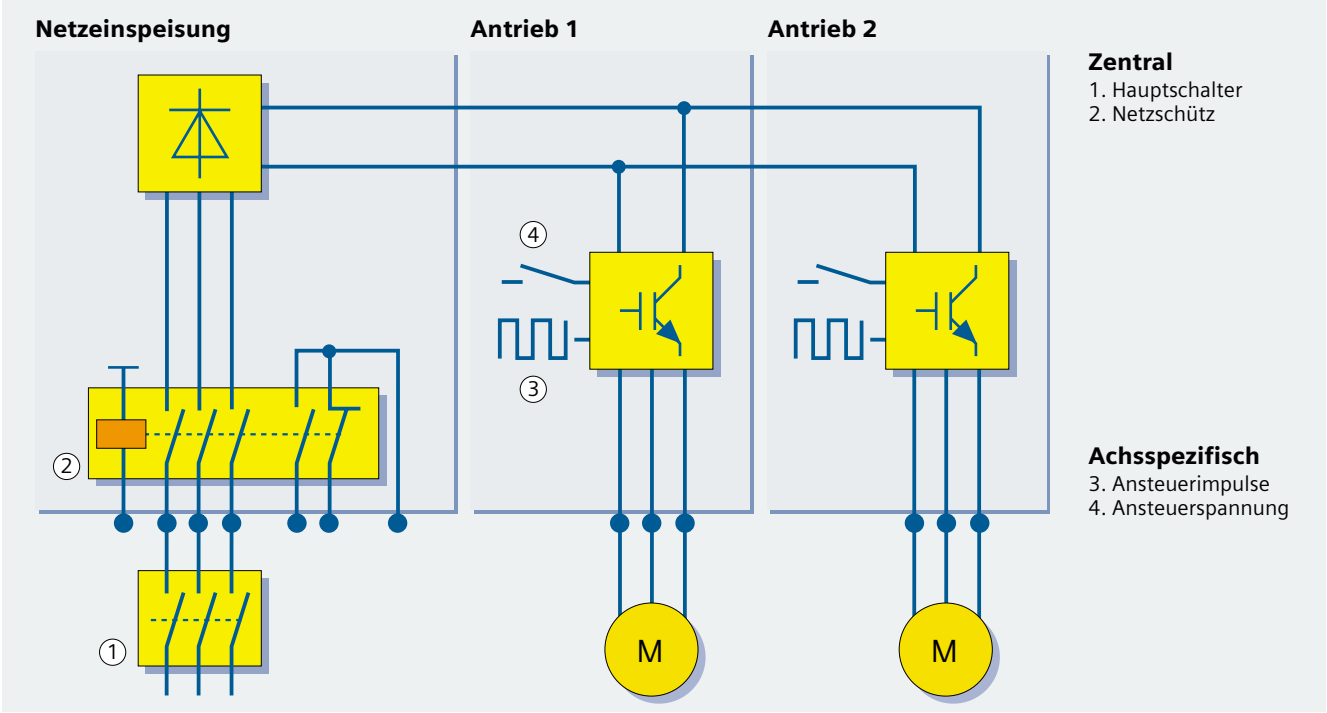


Bild 8/14
Sicherer Halt – elektronische, kontaktfreie Energieabtrennung

Die Bild 8/14 zeigt 4 grundsätzliche Möglichkeiten, um einen Motor drehmomentfrei zu schalten. Diese sind in ihrer Wirkungsweise unterschiedlich.

① **Hauptschalter:**
Wirkungsweise ⇨ zentral
Jede Maschine muss mindestens mit einem Schalter ausgerüstet sein, der eine galvanische Trennung zum Netz ermöglicht. Meist wird dies mit dem Hauptschalter realisiert. Diese Maßnahme schützt beim Arbeiten an spannungsführenden Teilen vor elektrischem Schlag. Der Schalter muss im ausgeschalteten Zustand gegen ungewolltes Einschalten gesichert werden.

② Integriertes Netzschütz:
Wirkungsweise ⇨ zentral
Mit dem Netzschütz in der Einspeisebaugruppe kann der gesamte Umrichter galvanisch vom Netz getrennt werden. Auf den Umrichter bezogen entspricht diese Maßnahme einem Stop der Kat. 0. In der Vergangenheit wurde mit dem integrierten Netzschütz bei Not-Halt der Umrichter/ Motor, in Verbindung mit einem Stop der Kat. 1, drehmomentfrei geschaltet. Eine galvanische Trennung ist für den Not-Halt jedoch nicht zwingend erforderlich.

(Siehe Systemhandbuch Kap. 1)

③ Impulslöschung im Steuersatz
Wirkungsweise ⇨ achsspezifisch
Die Impulslöschung über den Steuersatz ist die schnellste Möglichkeit, einen Antrieb achsspezifisch drehmomentfrei zu schalten. Diese Maßnahme ist jedoch für sich alleine noch nicht sicher.

④ Ansteuerspannung der Optokoppler
Wirkungsweise ⇨ achsspezifisch

Das Abschalten der Ansteuerspannung der Optokoppler bewirkt, dass im Fehlerfall noch anstehende Impulse des Steuersatzes nicht im Leistungsteil des Antriebes in ein Drehmoment umgesetzt werden können. Diese Maßnahme ist jedoch für sich alleine noch nicht sicher. Eine galvanische Trennung zwischen Umrichter-Zwischenkreis (600 V) und Motor ist damit nicht möglich. Dies ist für die „funktionale Sicherheit“ auch nicht erforderlich.

Fazit:

Die Maßnahmen 3 und 4 sind physikalisch entkoppelt und bilden gemeinsam eine wirkungsvolle und sichere Möglichkeit, die Impulse des Umrichters achsspezifisch zu löschen. Sie sind die Basis für den „sicheren Halt" und können vom Antrieb und der NC unabhängig angestoßen werden. Die Einbindung in zyklische Tests (Zwangsdynamisierung) runden das Konzept ab.

Somit wird aus einzelnen Maßnahmen ein sicheres Gesamtkonzept, das die Anforderungen für Not-Halt voll erfüllt. Das Abschalten des Netzschützes ist nicht mehr zwingend erforderlich.

Bei Arbeiten (z.B. Wartung, Service ...) an spannungsführenden Teilen ist immer eine galvanische Trennung zum Netz erforderlich.

Anmerkung bezüglich Emergency Stop (Not-Halt) in USA

Die NFPA 79 wurde aktuell überarbeitet und ist seit Mitte 2002 gültig. Darin sind zum ersten Mal entsprechend qualifizierte Software, Elektronik und Bussysteme für Emergency Stop erlaubt. Im Unterschied zur EU wird jedoch mit der Stop-Kategorie 1 abschließend noch eine galvanische Trennung verlangt. Dies lässt sich einfach als US-Variante projektieren.

Sicherer Betriebshalt – SBH

Die Funktion dient zur sicheren Überwachung der Stillstandsposition einer Achse oder Spindel. Die Antriebe befinden sich dabei voll funktionsfähig in Lageregelung oder Drehzahlregelung.

Funktionsmerkmale

- Achse bleibt in Regelung.
- Parametrierbares Stillstandstoleranzfenster.
- Projektierbare Stopreaktion beim Ansprechen der Überwachung (Stop B bzw. A).

Sichere Bremsrampe – SBR

Bei dieser Funktion liegt die Erwartungshaltung zugrunde, dass sich nach einer Stopanforderung die Istgeschwindigkeit verringern muss (Überwachung des Drehzahlverlaufs).

Mit Auslösen einer Stopanforderung wird die aktuelle Geschwindigkeit plus einer über das Maschinendatum vorgegebenen Geschwindigkeitstoleranz als Geschwindigkeitsgrenze aktiviert. Diese Grenze wird mit der aktuellen Geschwindigkeit verglichen (muss kleiner werden oder gleich bleiben) und zyklisch nachgeführt.
Dadurch wird ein erneutes Beschleunigen der Achse während des Bremsvorganges schnellstmöglich erkannt und eine Folgereaktion ausgelöst.

Funktionsmerkmale

- Schnellstmögliches Erkennen eines erneuten Beschleunigens der Achse während des Bremsvorganges.
- Die „sichere Bremsrampe" wird automatisch aktiviert, wenn ein Stop B oder C ausgelöst wurde.
- Beim Ansprechen der „sicheren Bremsrampe" wird direkt Stop A ausgelöst.

Beispiel Not-Halt

Die logische Verknüpfung von sicherheitsgerichteten Signalen und die erforderlichen Reaktionen erfolgen intern in sicherer Technik. Die elektrischen Antriebe werden sicher stillgesetzt und anschließend über die Elektronik von der Energie getrennt. Ein ungewollter Wiederanlauf wird ebenfalls sicher verhindert. Externe gefahrbringende Energien, wie z.B. Hydraulik oder Laser usw., können über sicherheitsgerichtete Ausgänge von der integrierten Not-Halt-Logik und nachgeschalteten Aktoren (Leistungsschütze, Ventile, ...) abgeschaltet werden. Das koordinierte, sichere Stillsetzen verhindert bzw. reduziert Folgeschäden (z.B. Crash) beim Abschalten und ermöglicht einen schnellen, einfachen Wiederanlauf.

Teststop

Mit dem Teststop wird bei jedem Überwachungskanal der gesamte Abschaltpfad mit den externen Beschaltungen getestet.

Bei der Durchführung des Tests werden die für die Stopfunktion zuständigen Komparatoren und Stopmodule der beiden Überwachungskanäle nacheinander durchlaufen. Zum Thema Zwangsdynamisierung siehe auch Abschnitt „Zwangsdynamisierung" bei SINUMERIK Safety Integrated.

Überwachung von Geschwindigkeit und Position

Sicher reduzierte Geschwindigkeit – SG

Die Funktion „sicher reduzierte Geschwindigkeit" dient zur sicheren Überwachung der Geschwindigkeit eines Antriebes.

Es wird dabei zyklisch im Überwachungstakt die aktuelle Geschwindigkeit des Antriebes mit dem über SGEs angewählten Geschwindigkeits-Grenzwert verglichen. Die Geschwindigkeits-Grenzwerte werden in speziellen Maschinendaten definiert.

Mit den Geschwindigkeits-Grenzwerten für SG1, SG2, SG3 oder SG4 können unterschiedliche Anwendungen bzw. Betriebszustände an der Maschine überwacht werden. Zusätzlich können die Grenzwerte SG2 und SG4 über „sicherheitsgerichtete Eingänge" (SGE) mit dem SG-Override jeweils in 16 Schritten (4 Bit) abgestuft werden. Die Eingabe erfolgt in % (1 bis 100%) und ist in einer Tabelle der Maschinendaten abgelegt. Somit stehen in Summe pro Antrieb 34 frei wählbare Geschwindigkeits-Grenzwerte zur Verfügung. Damit kann ein Personen- und Maschinenschutz im Einrichtbetrieb oder auch im Automatikbetrieb realisiert werden.

Anmerkung: Bei Schaltgetrieben muss die Anwahl der richtigen Getriebeübersetzung beachtet werden!

Funktionsmerkmale

- Sichere Überwachung der lastseitigen Geschwindigkeits-Grenzwerte.
- Anpassen der Überwachungs-Grenzwerte an verschiedene Betriebszustände (z.B. Test-, Einricht-, Automatikbetrieb).
- Projektierbare, SG-spezifische Stopreaktionen.

SG-spezifische Sollwertbegrenzung

Mit dieser Funktion wird erstmals neben dem Geschwindigkeitsistwert auch der Geschwindigkeitssollwert in die Betrachtung einbezogen. Die „SG-spezifische Sollwertbegrenzung" begrenzt den Sollwert automatisch auf den aktuell wirksamen Grenzwert der „sicher reduzierten Geschwindigkeit". Ändert sich dieser für einen Antrieb, wird die Sollwertbegrenzung automatisch nachgeführt. Arbeiten Antriebe im Verbund, so wirkt die Funktion auf alle gekoppelten Antriebe. Die Kontur bleibt somit immer erhalten.

Anwendungsbeispiel

- Beim Testen von NC-Programmen (Betriebsart 3), z.B. bei offener Schutztür. Es müssen nun keine testspezifischen Veränderungen an Programm-Parametern vorgenommen werden.
- Fährt man, z.B. über Verfahrtasten, in einen Sicherheitsbereich ein, bei dem niedrigere SG-Grenzwerte aktiv sind, wird nicht abgeschaltet, sondern automatisch auf den dort zulässigen Geschwindigkeitssollwert reduziert.

Funktionsmerkmale

- Die Sollwertbegrenzung wirkt 1-kanalig in der NCK.
- Wirksam beim Verfahren der Antriebe über Verfahrtasten oder beim Ablauf von NC-Programmen.
- Der Wert der Begrenzung liegt um einen einstellbaren Prozentwert unter dem aktiven SG-Grenzwert.
- Verzögerungsfreies, interpolatorisches Beschleunigen oder Abbremsen der beteiligten Achsen.
- Die Funktion wird nur ausgeführt, wenn der programmierte Sollwert oberhalb des aktiven SG-Grenzwertes liegt.
- Ist der programmierte Sollwert kleiner als der aktive SG-Grenzwert, fahren die Antriebe wie im Programm vorgegeben.

Sichere Software-Endschalter – SE

Durch die „sicheren Software-Endschalter" (SE) kann eine Arbeitsraum-/Schutzraumabgrenzung oder Verfahrbereichsbegrenzung achsspezifisch realisiert werden. Damit können z.B. Hardware-Endschalter an der Mechanik entfallen. Es sind zwei Endschalterpaare pro Achse verfügbar. Jedes Endschalterpaar besteht aus einem Plusschalter (SE1+ und SE2+) und einem Minusschalter (SE1– und SE2–). Über SGE kann zwischen dem SE1 und SE2 umgeschaltet werden.

Funktionsmerkmale

- Sicheres softwaremäßiges Festlegen und Auswerten von Endpositionen.
- Projektierbare Stopreaktion beim Überfahren von Endpositionen.
- Stopreaktion beim Überfahren von Endpositionen erfolgt softwareintern.

Sichere Software-Nocken – SN

Durch die Funktion „sichere Software-Nocken“ (SN) kann eine sichere Bereichserkennung achsspezifisch realisiert werden und damit die heutige „hardwaremäßige Lösung“ ersetzen.

Es sind 4 Nockenpaare (SN1 bis SN4) pro Achse verfügbar. Jedes Nockenpaar besteht aus einem Plusnocken (SN1+, SN2+, SN3+, SN4+) und einem Minusnocken (SN1–, SN2–, SN3–, SN4–). Jedes Nockensignal kann einzeln über Maschinendatum projektiert werden. Die Nockensignale werden über SGAs ausgegeben.

Funktionsmerkmale

- Sicheres softwaremäßiges Festlegen und Auswerten von Nockenpositionen.
- Definieren von Sicherheitsbereichen.
- SN-abhängiges, sicheres Umschalten von Sicherheitsfunktionen (z.B. sicheres positionsabhängiges Umschalten der SG-Stufen).

Verknüpfung sicherheitsgerichteter Prozess-Signale

Sichere programmierbare Logik – SPL

Die „sichere programmierbare Logik“ ermöglicht einen direkten Anschluss von sicherheitsgerichteten Sensoren und Aktoren und deren interne logische Verknüpfung. Die Verknüpfungslogik ist redundant in NC und in die interne PLC eingebunden. Damit lassen sich alle sicherheitsgerichteten Sensoren und Aktoren, wie z.B. Not-Halt- oder Verriegelungskonzepte für Schutztüren, über die Software von SINUMERIK Safety Integrated projektieren. In Verbindung mit dem „sicheren Halt“ kann der Not-Halt nun von der Auswertelogik bis zur Energieabtrennung kontaktfrei und in sicherer Technik realisiert werden. Die diskret aufgebauten Hardware-Schaltglieder können entfallen, was sich in einem vereinfachten Schaltschrankkonzept widerspiegelt. Lediglich Leistungsstellglieder (z.B. Schütze) zum direkten Ansteuern externer Aktoren sind erforderlich.

Funktionsmerkmale

- Universelle, programmierbare Logik in sicherer Technik
- Sofortige Aktivierung der Logik nach Hochlauf
- Zyklischer Ablauf unabhängig vom Anwenderprogramm
- Integrierter Timer für Zwangsdynamisierung
- Wirksam in allen Betriebsarten.

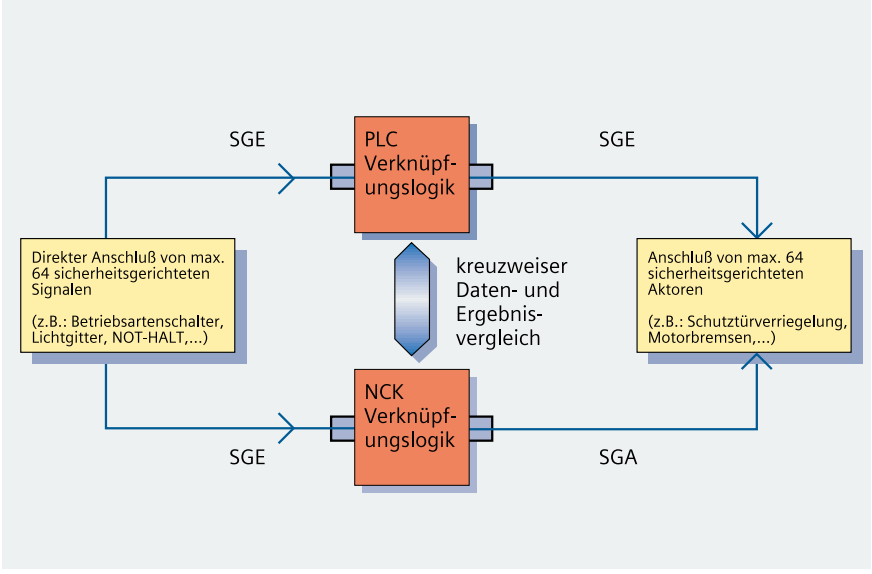


Bild 8/15
Grundstruktur – Sichere programmierbare Logik

Sicherheitsgerichtete Ein-/ Ausgangssignale – SGE/SGA

Die sicherheitsgerichteten Ein- und Ausgangssignale sind die Schnittstelle zum Prozess. Es sind digitale Signale, die 2-kanalig an das System gegeben werden bzw. vom System kommen. Die SGE/SGA müssen nicht unbedingt über Hardware-Klemmen geführt werden.

In Verbindung mit der SPL ist auch, je nach Anforderung, eine rein interne Verarbeitung als Softwaresignal möglich.

Funktionsmerkmale

- Sicherheitsfunktionen an- und abwählen
- Grenzwerte anwählen und umschalten
- Rückmelden von Status-Meldungen
- Ausgeben von Nockensignalen
- Direkter Anschluss von Sensoren
- Direkter Anschluss von Aktoren.

Absturzsicherung bei Vertikalachsen

Allgemeine Anforderungen

Achsen bzw. Mechaniken können, bei abgeschalteten Antrieben, durch die Schwerkraft nach unten fallen. Bei vertikalen Linearachsen (hängende Achsen) oder bei Rundachsen bzw. Spindeln mit asymmetrischer Gewichtsverteilung kann somit eine gefahrbringende Bewegung entstehen. Daher müssen diese Achsen bzw. Mechaniken durch geeignete Maßnahmen sicher im Stillstand gehalten werden. Maßnahmen hierzu können z.B. sein:

a) zeitweise aktiv
Haltebremse
Betriebsbremse
elektrischer Antrieb

b) dauernd aktiv
mechanischer Gewichtsausgleich

c) in Ausnahmen aktiv
Steckbolzen
Unterbauung/Stütze

Die Auswahl der Maßnahmen ist abhängig von der Art der Arbeit, die im Gefahrenbereich ausgeführt werden soll. Wird direkt unter der hängenden Last gearbeitet, oder nur im Nahbereich? Auch die Aufenthaltsdauer im Gefahrenbereich muss bei der Konzeption berücksichtigt werden, was eventuell eine Kombination von mehreren Maßnahmen erforderlich macht. Basis hierfür ist immer die Gefahrenanalyse, die für jede Maschine durchgeführt werden muss. Das Gesamtkonzept muss so ausgelegt sein, dass es den Anforderungen für den Personenschutz nach EG-Maschinenrichtlinie genügt.

Anmerkung:

Bei Arbeiten an spannungsführenden Teilen (außer Schutzkleinspannung) ist immer eine galvanische Trennung vom Netz notwendig.

Anforderungen aus dem BG Merkblatt (EM II, Mainz)

In diesem Merkblatt sind die Anforderungen an Maschinen mit entsprechendem Gefahrenpotenzial beschrieben. Anbei die wichtigsten Anforderungen als Auszug:

- Sicheres, redundantes Haltesystem zur "Absturzsicherung an Vertikalachsen"
- Test der mechanischen Bremsen (Steuerungskategorie 2 nach EN 954-1)
- Schutz vor ungewolltem Wiederanlauf des elektrischen Antriebes (Steuerungskategorie 3 nach EN 954-1)
- Abnahmetest mittels Formblatt

Das aktuelle Dokument kann im Internet unter
www.smbg.de/Sites/downloads/005-MFS-A04_Vertikalachsen.pdf
eingesehen werden.

Konzept zur Absturzsicherung an Vertikalachsen

Die bereits vorhanden Systeme, elektrischer Antrieb und mechanische Bremse, bilden zusammen das sichere, redundante Haltesystem. Das Sicherheitskonzept von SINUMERIK Safety Integrated bindet diese Standardkomponenten so ein, dass ihre Wirkung sicherheitsgerichtet ist.

1. Sicherer Antrieb erzielt durch Sicherheitsfunktionen wie z.B.:
   - „sicherer Halt"
   - „sicherer Betriebshalt"
   - „sicher reduzierte Geschwindigkeit"

2. Sichere Bremsenfunktion erzielt durch das "sicheres Bremsenmanagement" mit den Teilfunktionen:
   - „sichere Bremsenansteuerung"
   - „sicherer Bremsentest"

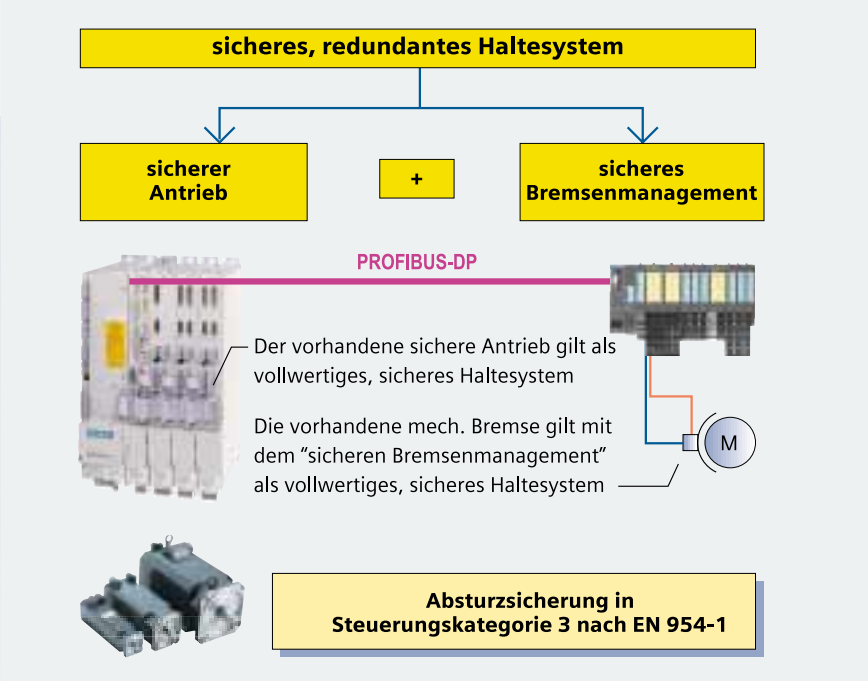

sicheres, redundantes Haltesystem
sicherer Antrieb
+
sicheres Bremsenmanagement
PROFIBUS-DP
Der vorhandene sichere Antrieb gilt als vollwertiges, sicheres Haltesystem
Die vorhandene mech. Bremse gilt mit dem "sicheren Bremsenmanagement" als vollwertiges, sicheres Haltesystem
M
Absturzsicherung in Steuerungskategorie 3 nach EN 954-1

Bild 8/16
Absturzsicherung an Vertikalachsen

Der sichere Antrieb bildet das 1. Haltesystem und ist überwiegend aktiv - die mechanische Bremse bildet, als sichere Bremsenfunktion, das 2. Haltesystem und befindet sich (geöffnet) im Standby-Modus.

Bei einem Ausfall des Antriebes wird die Bremse automatisch und sicher aktiviert und übernimmt das Halten der Mechanik. Der Einsatz einer zweiten Bremse ist nicht zwingend erforderlich. Damit steht zum Thema „Absturzsicherung an Vertikalachsen" (sowie Rundachsen bzw. Spindeln mit asymmetrischer Gewichtsverteilung) erstmals eine umfassende und durchgängige Lösung zur Verfügung.

Das Risiko bei Arbeiten an hängenden Lasten wird mit dieser Funktionalität deutlich reduziert und leistet somit einen weiteren Betrag zum Personenschutz. Darüber hinaus werden Maschinenschäden durch fallende Achsen weitgehend vermieden und es wird die Verfügbarkeit von Maschinen und Anlagen erhöht.

Das sichere redundante Haltesystem bietet je nach Anforderung folgende Einsatzmöglichkeiten:

1. Der Antrieb ist aktiv, die Bremse ist geöffnet und im Standby-Modus

   Zielsetzung: Durchsackweg minimieren auf < 25 mm
   - der Antrieb kann sich bewegen oder er steht
   - automatisches und sicheres Schließen der Bremse, sobald der Antrieb, z.B. durch einen Systemfehler, ausfällt

   Ergebnis:
   In Abhängigkeit von Geschwindigkeit, Bewegungsrichtung, Systemreaktionszeit, Bremsenschließzeit und Reibung der Mechanik kommt es zu einem nicht vermeidbaren Durchsacken der Vertikalachse.

2. Der Antrieb und die Bremse sind gleichzeitig aktiv (Antrieb mit adaptierten Regelparametern / Filtern)

   Zielsetzung: Durchsackweg minimieren auf < 1 mm
   - der Antrieb steht, die Bremse ist geschlossen
   - automatische Meldung, sobald eines der beiden Haltesysteme ausfällt
   - das noch intakte Haltesystem übernimmt nun alleine das Halten der Mechanik

Ergebnis:
Es kommt zu keinem, für den Personenschutz nennenswerten, Durchsacken der Vertikalachse.

Anmerkungen:

- Abnahmeprotokoll
  Im Abnahmeprotokoll ist der Durchsackweg zu messen und zu protokollieren!

- Betriebsbedingtes Abschalten der Antriebe

Der Antrieb wird auch unabhängig von Systemfehlern betriebsbedingt abgeschaltet, z.B. bei Not-Halt. Hierbei wird die Bremse geschlossen, bevor der Antrieb abgeschaltet wird und die Vertikalachse gezielt in die mechanische Klemmung überführt. Da es sich hierbei um einen gezielten Ablauf handelt, kommt es an der Vertikalachse zu keinem, für den Personenschutz nennenswerten, durchsacken (< 1 mm).

Sicheres Bremsenmanagment - SBM

Die Zuverlässigkeit der mechanischen Bremse ist ein wesentlicher Bestandteil bei der Absturzsicherung an Vertikalachsen. Untersuchungen von Unfällen haben ergeben, dass sowohl Fehler in der Ansteuerung als auch in der Mechanik der Bremse verantwortlich für den Absturz der Vertikalachsen waren. Die Analyse zeigt auch, dass durch den Einsatz von Sicherheitstechnik die Unfälle vermeidbar gewesen wären.

Wir nehmen dies zum Anlass, und bieten unseren Kunden mit dem „sicheren Bremsenmanagement" eine Lösungsmöglichkeit an.

Das „sichere Bremsenmanagement" SBM (Safe Brake Management)besteht aus zwei Funktionsteilen:

1. sichere Bremsenansteuerung
   SBC (Safe Brake Control)

2. sicherer Bremsentest
   SBT (Safe Brake Test)

Bei den heute gebräuchlichen Bremsen handelt es sich nicht um sicherheitsgerichtete Bauteile. Durch die Einbindung der Standard-Bremse (betriebsbewährtes Bauteil) in das Sicherheitskonzept von SINUMERIK Safety Integrated wird daraus eine sichere Bremsenfunktion.

Die Bremse wird sicher angesteuert und einer Zwangsdynamisierung unterzogen. Da es für das Haltemoment kein Rückmeldesignal gibt, sind erweiterte Testmaßnahmen erforderlich. Der sichere Bremsentest kann diese Anforderung erfüllen. Mit diesen erweiterten Testmaßnahmen können Fehler in der Ansteuerung und an der Mechanik der Bremse aufgedeckt werden.

In Abhängigkeit vom Ergebnis der Gefahrenanalyse ergeben sich für den Anbau der Bremse verschiedene Varianten:

1. Eine Bremse im Motor
   Übertragungsglieder mit
   Überlastfaktor > 2
   (BG EM II, Mainz)

2. Eine Bremse an der Last
   Übertragungsglieder mit
   Überlastfaktor < 2

3. Eine Bremse im Motor
   besondere Anforderungen
   und eine Bremse an der Last

Im Zweifelsfalle ist die Montage der Bremse an der Last, z.B. an der Linearführung, der Montage im Motor vorzuziehen.

Sichere Bremsenansteuerung

Die Bremse (Betriebs-/oder Haltebremse) wird in Steuerungs-Kategorie 3 (nach EN 954-1) sicher elektrisch angesteuert. Die Ansteuerung erfolgt zweikanalig (P/M-schaltend) mit:

- sicherheitsgerichteten Ausgängen mit getrennter Hardware von PLC und NC

- fehlersicheren Ausgängen der F-DO in ET 200S PROFIsafe

Mit beiden Varianten ist es möglich, Fehler auf den Ansteuerleitungen, wie z.B. Kurzschlüsse, Leitungsbruch usw. aufzudecken. Auch wenn ein Kanal ausfällt, kann die Bremse weiterhin angesteuert werden.

Anmerkung:

Relaiszwischenstufen erhöhen die Reaktionszeit bei der Ansteuerung der Bremse – der Durchsackweg der Vertikalachse erhöht sich somit. Daher sollte, wenn möglich, eine direkte, elektronische Ansteuerung bevorzugt werden – dies ist bis 2 A möglich.

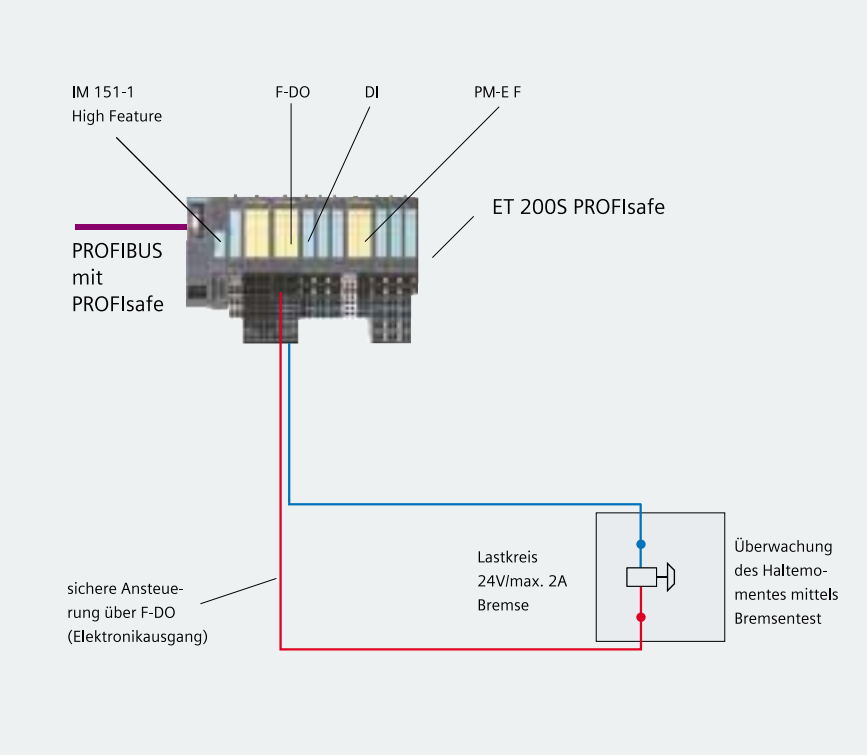


Bild 8/17
Sichere Bremsenansteuerung

Sicherer Bremsentest

Der sichere Bremsentest prüft zyklisch, ob das erwartete Haltemoment noch verfügbar ist. Der Antrieb fährt dabei gezielt gegen die geschlossene Bremse und belastet diese mit dem Testmoment - im „Gutfall" ohne eine Achsbewegung auszuführen. Wird jedoch eine Achsbewegung festgestellt, so ist davon auszugehen, dass das Haltemoment der Bremse nicht mehr ausreicht um die Vertikalachse zu halten. Der Test wird abgebrochen und eine Fehlermeldung ausgegeben. Anschließend ist eine sichere Position anzufahren und die Vertikalachse abzusetzen oder mit Bolzen abzustecken – dies kann auch automatisch erfolgen. Die Schutztür bleibt so lange verriegelt, bis die „Absetzposition" angefahren wurde. Diese Abfrage kann über "sichere Software-Nocken" realisiert werden. Sind alle Bedingungen erfüllt, muss eine Wartung der Bremse erfolgen.

Der sichere Bremsentest wird im Rahmen der Zwangsdynamisierung vor dem Test der Abschaltpfade durchgeführt. Wird ein Defekt an der Bremse erkannt wird der Test der Abschaltpfade, der eine Impulslöschung zur Folge hätte, nicht mehr angestoßen und eine Fehlermeldung erzeugt.

Der sichere Bremsentest ist in Kategorie 2 realisiert.

Anmerkung zur Stop-Kategorie 1 nach EN 60204 bei Not-Halt

Die Norm fordert nach dem generatorischen Bremsen der elektrischen Antriebe, eine Energietrennung als Schutz vor ungewolltem Wiederanlauf. Not-Halt hat jedoch als Ziel den Schutz vor gefahrbringender Bewegung und nicht den Schutz vor elektrischem Schlag. Die EN 60204 berücksichtigt nicht, dass sichere Antriebe für Not-Halt mit Stop-Kategorie 2 mindestens die gleiche Qualität garantieren können. Sichere Antriebe überführen bei Stop-Kategorie 2, nach dem Stillsetzen, in den „sicheren Betriebshalt" und bleiben voll funktionsfähig in Regelung.

Zur Verdeutlichung folgendes Szenario mit konventioneller Technik:

1. An einer Vertikalachse ist das Haltemoment der mechanischen Haltebremse durch einen Fehler (Ansteuerung/Mechanik) gleich Null. Not-Halt ist nach EN 60204 mit Stop-Kategorie 1 projektiert.

2. Bei konventionellen Sicherheitskonzepten werden Fehler in der Ansteuerung der Bremse sowie in der Bremsenmechanik nicht aufgedeckt – es handelt sich somit um einen „schlafenden Fehler".

3. Ein Bediener betätigt nun den Not-Halt!
   Ergebnis:
   Da die Haltebremse defekt ist, und der Antrieb mit Stop-Kategorie 1 von der Energie getrennt wird, fällt die Vertikalachse nach unten und erzeugt in Verbindung mit Not-Halt eine gefahrbringende Bewegung!

Gleiches Szenario mit sicheren Antrieben

1. An einer Vertikalachse ist das Haltemoment der mechanischen Haltebremse durch einen Fehler in der Mechanik gleich Null (ein Fehler in der Bremsenansteuerung wird direkt aufgedeckt und die Bremse über den zweiten Kanal geschlossen). Not-Halt ist nach EN 60204 mit Stop-Kategorie 1 projektiert.

2. Der Fehler wird durch den Bremsentest aufgedeckt. Eine entsprechende Fehlermeldung wird angezeigt. Die Schutztür bleibt verriegelt und es muss eine sichere Position angefahren werden.

3. Ein Bediener betätigt nun, vor Erreichen der sicheren Position, den Not-Halt!
   Ergebnis:
   Trotz aktiviertem Not-Halt wird der Antrieb mit der defekten Bremse nicht von der Energie getrennt, sondern sicher stillgesetzt und anschließend der Stillstand mit dem sicheren Betriebshalt sicher überwacht. Es entsteht keine gefahrbringende Bewegung.

Integriertes und teilautomatisiertes Abnahmeprotokoll

Bei jeder Antriebssteuerung wird das Systemverhalten über einstellbare Parameter an die Anforderungen der jeweiligen Maschine angepasst. Dabei werden z.B. maximal zulässige Geschwindigkeiten oder das Bremsverhalten beim Stillsetzen eines Antriebs festgelegt. Hierbei können sowohl bei der Projektierung, wie auch bei der Eingabe der Parameter über einen PC oder ein Programmiergerät, Fehler gemacht werden. Deshalb sind im Rahmen der Inbetriebnahme alle Sicherheitsfunktionen elektrischer Antriebssysteme durch einen Abnahmetest der Maschine zu testen und zu protokollieren. Dies muss, unabhängig davon, ob die Sicherheitsfunktionen unter Verwendung von Steuerungen mit integrierter Sicherheit oder unter Verwendung von externen Überwachungseinrichtungen realisiert sind, geschehen.

Es wird zwischen einem vollständigen und einem partiellen Abnahmetest unterschieden. Bei einem vollständigen Abnahmetest sind dabei alle vorgesehenen Sicherheitsfunktionen (z.B. Einhalten der Grenzwerte, Funktionen der Befehlsgeber, Funktionen der Aktoren) zu überprüfen. Bei dem Test wird dabei die gesamte Fehlerreaktions-Kette, vom Sensor über die Steuerung, bis hin zum Aktor, durchlaufen und die korrekte Wirkungsweise der Sicherheitsfunktionen überprüft. Dies gilt für alle elektrischen Antriebssysteme in Maschinen. Beim partiellen Abnahmetest müssen nur die sicherheitsrelevanten Parameter getestet werden, die gegenüber dem vollständigen Abnahmetest geändert wurden oder neu hinzugekommen sind.

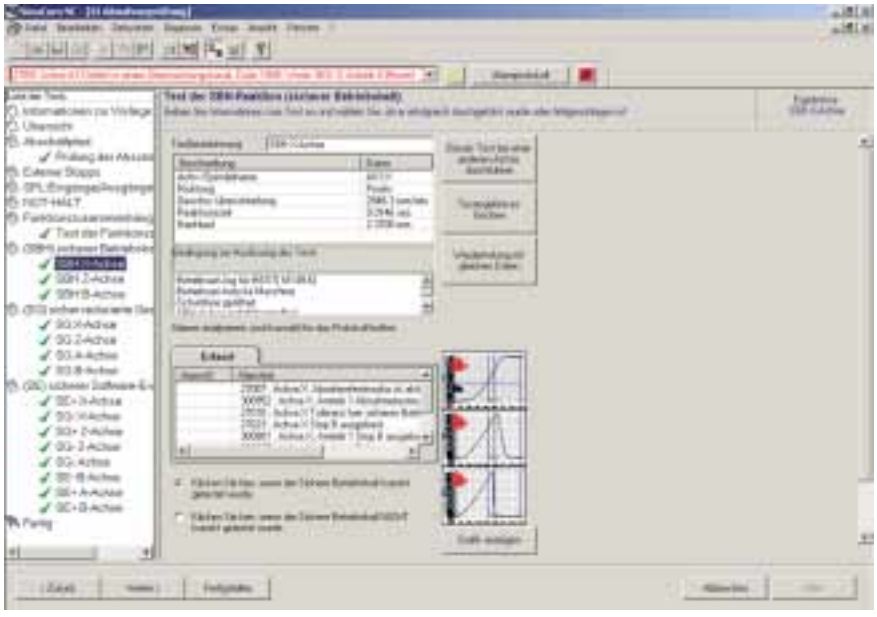


Bild 8/18
Abnahmetest für den sicheren Betriebshalt

Mit dem integrierten Abnahmetest steht dem Maschinenhersteller ein Tool zur Verfügung, mit dem dieser Test halbautomatisch und bedienergeführt realisiert werden kann. Dabei werden die Trace-Funktionen automatisch konfiguriert. Das automatisch generierte Abnahmeprotokoll ist sowohl für den Maschinenhersteller als auch für den Maschinenbetreiber ein Beleg für die geprüfte funktionale Sicherheit der Maschine. Die mit dem geführten Abnahmetest erzielbare Zeitersparnis ist ganz erheblich.

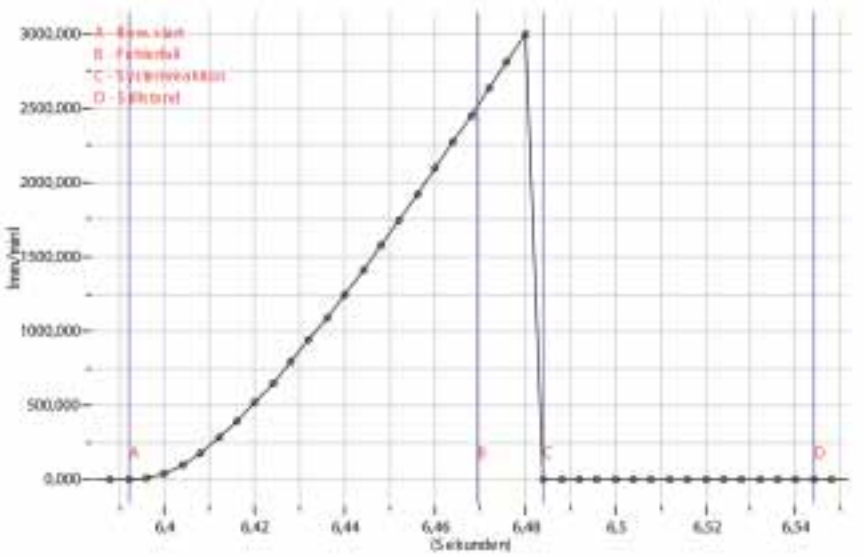


Bild 8/19
Sollgeschwindigkeit

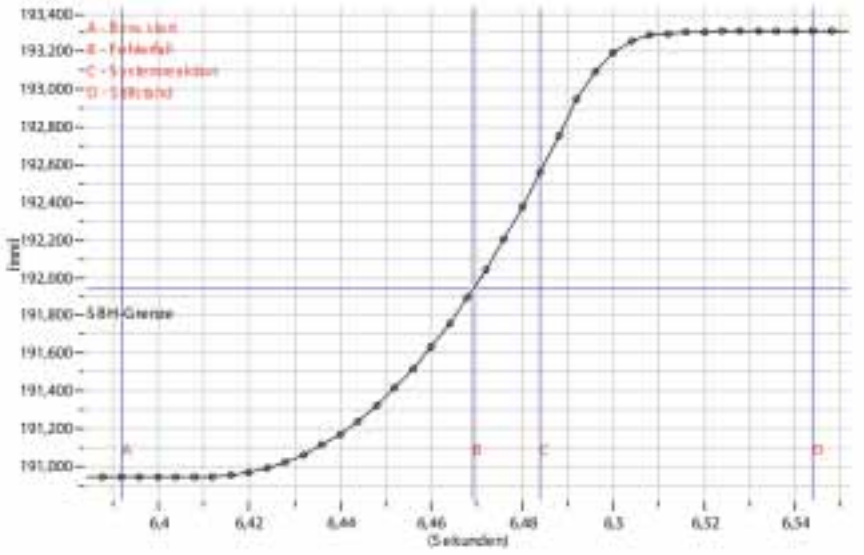


Bild 8/20
Istposition

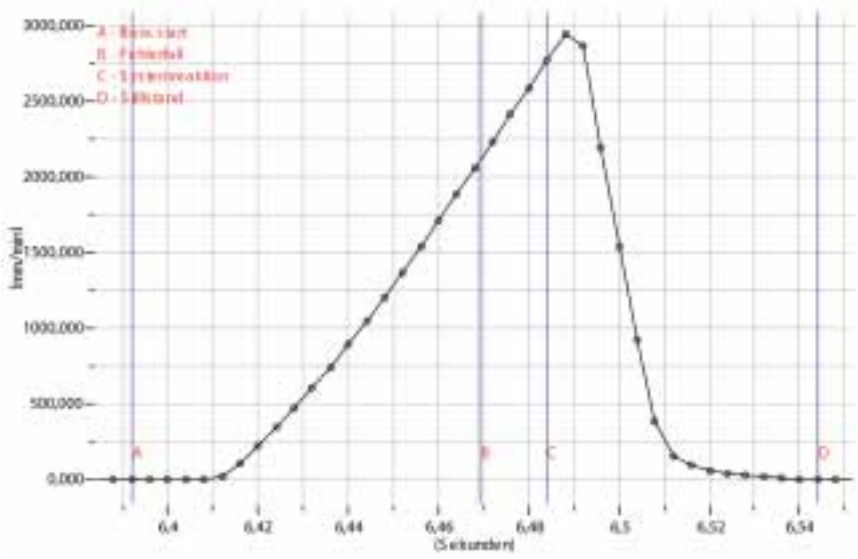


Bild 8/21
Istgeschwindigkeit

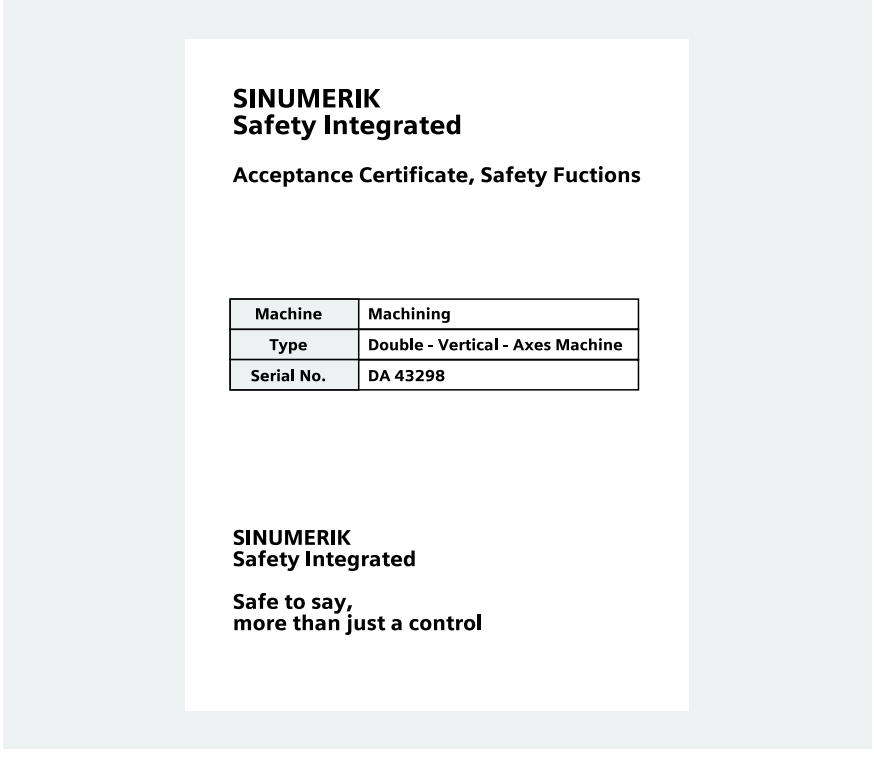


Bild 8/22
Zertifikat für Abnahmetest

Zwangsdynamisierung bei SINUMERIK Safety Integrated

Die Zwangsdynamisierung dient der Fehleraufdeckung in der Software und Hardware der beiden Überwachungskanäle. Dazu müssen die sicherheitsrelevanten Teile in den beiden Kanälen mindestens einmal innerhalb eines definierten Zeitrahmens in allen sicherheitsrelevanten Verzweigungen durchlaufen werden. Ein Fehler in einem Überwachungskanal führt zu Abweichungen und wird durch den kreuzweisen Datenvergleich (KDV) erkannt.

Die Zwangsdynamisierung des Abschaltpfades (Teststop) muss vom Anwender ausgelöst oder automatisiert in den Prozess eingebunden werden, und zwar beispielsweise:

- bei stillstehenden Achsen nach dem Einschalten der Anlage
- beim Öffnen der Schutztür
- in einem vorgegebenen Rhythmus (z.B. im 8-Stunden-Rhythmus)
- im Automatikbetrieb, zeit- und ereignisabhängig

Zur Zwangsdynamisierung gehört auch der Test der sicherheitsrelevanten Sensoren und Aktoren. Dabei wird die gesamte Signalkette, inklusive der „sicheren programmierbaren Logik" (SPL), auf ihre Funktionsfähigkeit überprüft.

Anmerkung:

Für die Dauer des Automatikbetriebes (also bei geschlossener Schutztür) ist der feste 8-Stunden-Rhythmus nicht zwingend vorgeschrieben. Hierbei kann die Zwangsdynamisierung nach Ablauf der 8 Stunden mit dem nächsten Öffnen der Schutztür verknüpft werden. Durch den kreuzweisen Datenvergleich werden Fehler in den sicherheitsrelevanten Daten der beiden Überwachungskanäle aufgedeckt. Bei „veränderlichen" Daten gibt es über Maschinendaten festgelegte Toleranzwerte. Innerhalb dieser Toleranzen dürfen die Ergebnisse der beiden Kanäle abweichen, ohne dass eine Reaktion ausgelöst wird. Ein Beispiel ist die Toleranz für kreuzweisen Datenvergleich der Ist-Positionen. Fehler, die durch Zwangsdynamisierung bzw. kreuzweisen Vergleich aufgedeckt werden, führen zu einer Stop-F-Reaktion und lösen weitere Stopreaktionen aus (siehe Abschnitt „Stopreaktionen").

Sensor-/Aktor-Einbindung - Grundlagen

Zur sicheren Einbindung von Sensoren und Aktoren müssen deren Prozess-Signale zur weiteren Verarbeitung der „sicheren programmierbaren Logik" SPL zugeführt werden.

Hierzu gibt es folgende Anschluss-Varianten:

1. über getrennte Hardware von PLC und NC in Schutzart IP20
2. über PROFIsafe mit Peripherie-Baugruppen ET 200S PROFIsafe in Schutzart IP20
3. über PROFIsafe als direkte, sichere Kommunikation mit einem sicheren PROFIsafe-Sensor / -Aktor

Das gilt für Prozess-Signale von:

- Sensoren, wie z.B. Schalter, Schutztürkontakte, Not-Halt-Taster, Lichtvorhänge, Laser-Scanner
- Aktoren, wie z.B. Lastschütze, Ventile, Verriegelungsmagnete, Bremsen

Diese werden ohne externe Auswertegeräte direkt angeschlossen und an die „SINUMERIK Safety Integrated"-Plattform übertragen.

Anmerkungen zur Mechanik des Sensors

Folgende Fälle sind zu unterscheiden:

1. Der Sensor (z.B. Schutztürverriegelung) ist ein Sicherheitsbauteil und zertifiziert. Damit kann ein Fehlerausschluss erfolgen - es sind keine weiteren Maßnahmen erforderlich.
2. Der Sensor ist ein betriebsbewährtes Bauteil nach EN 954-2
   Ein Fehlerausschluss kann unter folgenden Bedingungen erfolgen:
   - Regelmäßige Wartung nach Vorgabe des Herstellers
   - Regelmäßiger Austausch des Sensors nach Ablauf der Produktlebensdauer
   - Die Fehleraufdeckung erfolgt durch die nachgeschaltete Elektronik über zyklische Tests mittels Dynamisierung durch den Prozess (z.B. Schutztür), oder durch Zwangsdynamisierung.
3. Der Sensor ist kein betriebsbewährtes Bauteil nach EN 954-2.
   Es kann kein Fehlerausschluss erfolgen.
   - Die beiden signalgebenden Elemente (z.B. Schaltkontakte eines Tasters) des Sensors müssen mechanisch entkoppelt sein – oder es werden zwei separate Sensoren eingesetzt.
   - Die Fehleraufdeckung erfolgt durch die nachgeschaltete Elektronik über zyklische Tests mittels Dynamisierung durch den Prozess (z.B. Schutztür), oder durch Zwangsdynamisierung.

Anmerkungen zur Mechanik des Aktors

Folgende Fälle sind zu unterscheiden:

4. Der Aktor (z.B. sicherer Motorstarter) ist ein Sicherheitsbauteil und zertifiziert. Damit kann ein Fehlerausschluss erfolgen - es sind keine weiteren Maßnahmen erforderlich.

5. Der Aktor ist ein betriebsbewährtes Bauteil nach EN 954-2 (z.B. Ventil) Ein Fehlerausschluss kann unter folgenden Bedingungen erfolgen:

   - Regelmäßige Wartung nach Vorgabe des Herstellers
   - Regelmäßiger Austausch des Aktors nach Ablauf der Produktlebensdauer
   - Die Fehleraufdeckung erfolgt über das Rückmeldesignal aus dem Prozess und zyklischen Tests mittels Dynamisierung durch den Prozess oder durch Zwangsdynamisierung.

6. Der Aktor ist ein Standardbauteil Es kann kein Fehlerausschluss erfolgen.

   - Es sind zwei separate, mechanisch entkoppelte Aktoren erforderlich.
   - Die Fehleraufdeckung erfolgt über das Rückmeldesignal aus dem Prozess und zyklischen Tests mittels Dynamisierung durch den Prozess oder durch Zwangsdynamisierung.

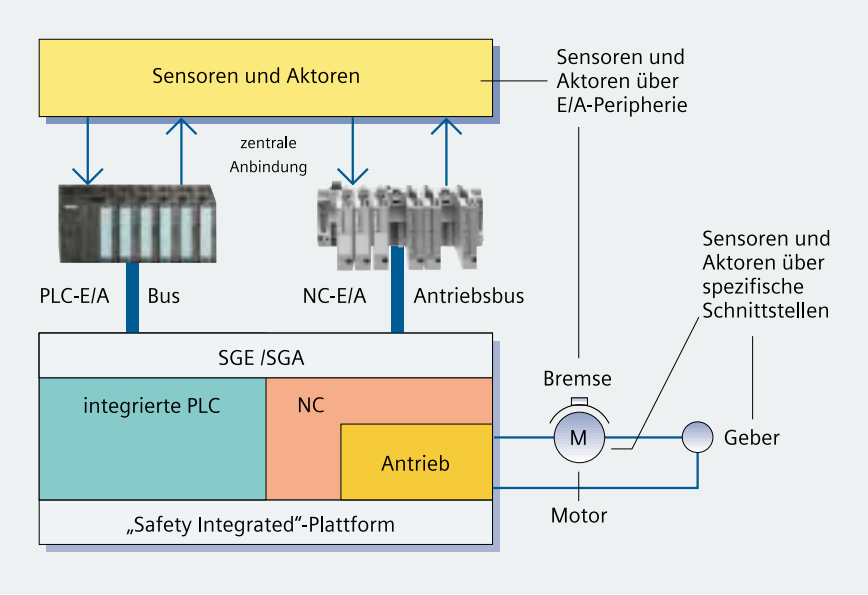


Bild 8/23
Sensor-Aktor-Einbindung über S7 Peripherie und dem DMP Modul der NC

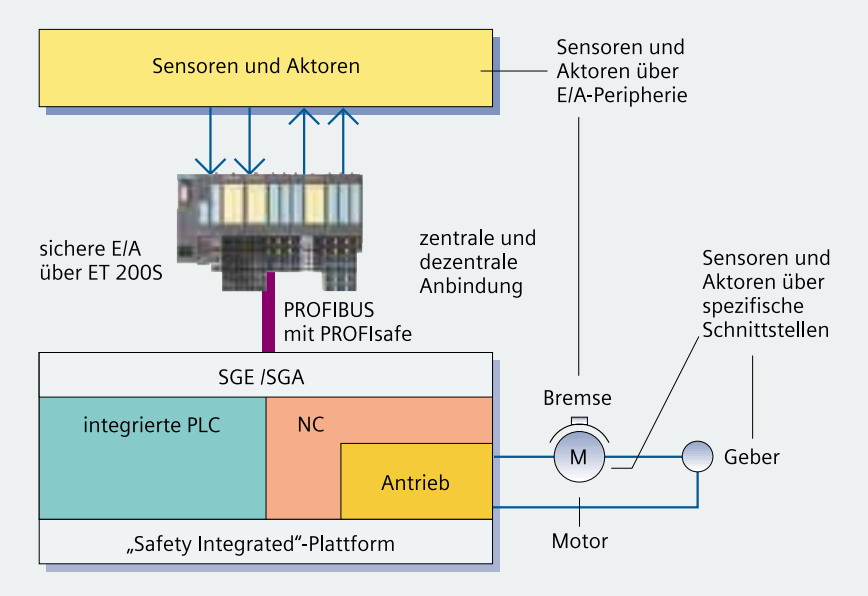


Bild 8/24
Sensor-Aktor-Einbindung über ET 200S PROFIsafe

Sensor-/Aktor-Einbindung über getrennte Hardware E/A von PLC und NC

Grundstruktur

Die Sensoren und Aktoren werden ohne externe Auswertegeräte direkt an die Standard-Peripheriebaugruppen von PLC und NC angeschlossen. Die Signale stehen dann, über separate Busse, der „SINUMERIK Safety Integrated"-Plattform zur Verfügung. Bei der Sensor-Einbindung erfolgt immer eine 2-von-2-Auswertung.

Merkmale

- Standard E/A-Baugruppen
- Getrennte Hardware-Kanäle
- Separate Busse

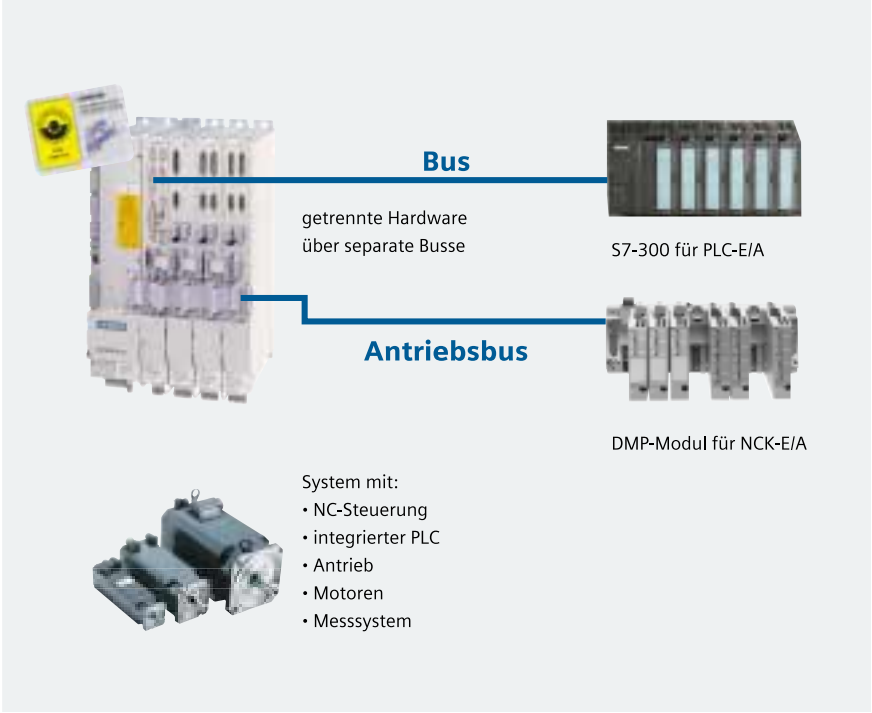


Bild 8/25
Sensor-Aktor-Einbindung über S7 Peripherie und dem DMP Modul der NC

Sensor-Aktor-Einbindung nach dem 3-Klemmen-Konzept

Sensor-Einbindung

Bei Sensoren, die über die E/A-Peripherie von PLC und NC angeschlossen werden, kann man als Grundschema von einem 3-Klemmen- Konzept ausgehen. Werden von einem Sensor die Signale 2-kanalig gelesen, dann ist ein 1-kanaliger Test-Ausgang für Steuerungskategorie 3 ausreichend. Damit sind für die sicherheitsgerichtete Einbindung des Sensors 3 Klemmen an der E/A-Peripherie erforderlich.

2 Eingänge + 1 Testausgang

Aktor-Einbindung

Bei Aktoren, die über die E/A-Peripherie von PLC und NC angeschlossen werden, kann man auch als Grundschema von einem 3-Klemmen-Konzept ausgehen. Wird ein Aktor 2-kanalig angesteuert, so ist ein 1-kanaliges Rücklesen des Prozesssignals für Steuerungskategorie 3 ausreichend. Damit sind für die sicherheitsgerichtete Einbindung des Aktors auch 3 Klemmen an der E/A-Peripherie erforderlich.

2 Ausgänge + 1 Testeingang

Querschluss-Sicherheit

Sind die Anschlussleitungen geschützt im Schaltschrank oder in Anlagenteilen verlegt, so kann davon ausgegangen werden, dass ein Fehler (Kurzschluss, Querschluss, ...) höchst unwahrscheinlich ist. Wie in der Norm EN 954-2 festgelegt, kann in diesem Fall für die Anschlussleitung ein so genannter Fehlerausschluss angenommen werden. Eine Auslegung des Sensors nach dem 3-KlemmenKonzept ist damit völlig ausreichend.

Die Maßnahmen zur Querschluss-Sicherheit sind unabhängig von der Steuerungs-Kategorie (3 oder 4).

Sicherheitsgerichtete Hardware-Eingangssignale

Grundsätzlich müssen alle sicherheitsgerichteten Prozess-Signale (Sensoren wie z.B. Not-Halt, Schutztür, Lichtvorhang, ...) redundant bereitgestellt und getrennt als „sicherheitsgerichtete Eingänge" (SGE) auf die 2-kanalige Eingangsperipherie von PLC und NC aufgelegt werden. Dabei dürfen die Eingangsklemmen nicht direkt gebrückt werden.

Anwendungsbeispiel: Not-Halt

Merkmale

- Der Sensor wird von einem Testausgang der PLC mit 24 V über einen Wurzelanschluss angesteuert und über die beiden Eingangs-Kanäle 1 und 2 an die sicherheitsgerichtete Steuerung geführt.
- In Verbindung mit dem kreuzweisen Datenvergleich und der Zwangsdynamisierung können Fehler (P- und M-Kurzschluss) in den Anschlussleitungen aufgedeckt werden.
- Ein reiner Querschluss zwischen den beiden Eingängen von Kanal 1 und 2 kann mit dem 3-Klemmen-Konzept nicht aufgedeckt werden.

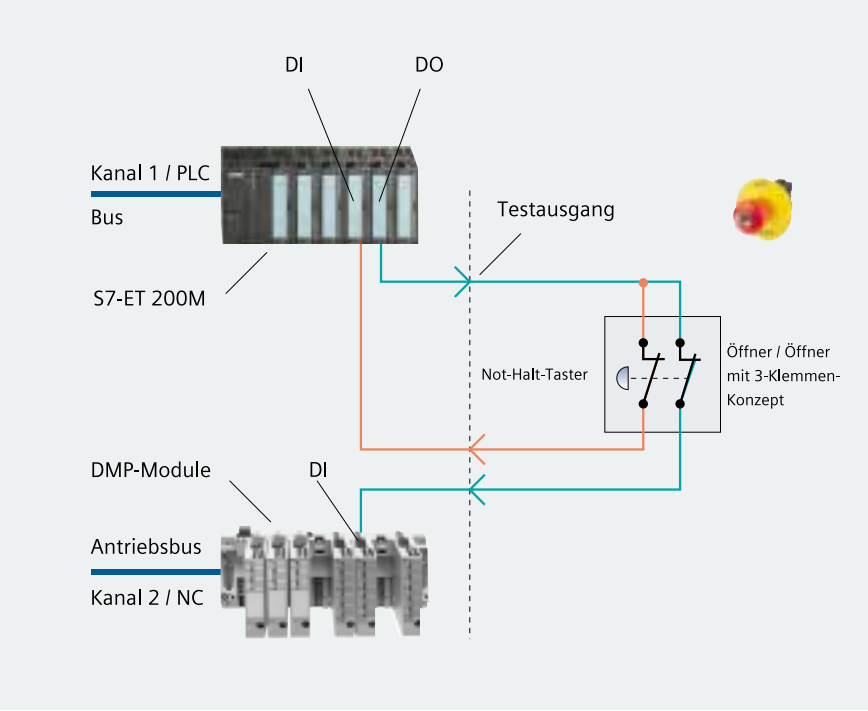


Bild 8/26
Sensor-Einbindung mit 3-Klemmenkonzept – Beispiel Not-Halt

Es ist sicherzustellen, dass der Signalzustand der „sicherheitsgerichteten Eingänge" nicht differiert. Abhängig vom Toleranz-Timer (ca. < 1 Sek.) spricht beim Überschreiten der Toleranzzeit eine Überwachung an und ein sicheres Stillsetzen der Maschine wird automatisch ausgeführt.

Anmerkung 1:

Bei Sensoren, die reine Elektronikausgänge, also keine kontaktbehaftete Technik anbieten, wie z.B. teilweise bei Lichtvorhängen möglich, bleibt die Beschaltung an den PLC- und NC-Eingängen gleich. Der Testausgang der PLC wird jedoch direkt mit dem speziellen Testeingang am Sensor verbunden. Das 3-Klemmen-Konzept bleibt dabei grundsätzlich erhalten.

Anmerkung 2:

Wenn kein Sicherheitsbauteil (z.B. Not-Halt-Taster) als Sensor eingesetzt wird, müssen die beiden signalgebenden Elemente (z.B. Schaltkontakte beim Taster) mechanisch entkoppelt sein.

Sensor-Einbindung nach dem 4-Klemmen-Konzept

Kann der Schutz der Anschlussleitungen gegen Quetschung nicht durchgängig gewährleistet werden (z.B. Kabel für Bedienhandgerät/Programmierhandgerät), oder werden durch die Applikation höhere Anforderungen gestellt, so muss in der Gefahrenanalyse mit einem reinen Querschluss (kein P- oder M-Kurzschluss) gerechnet werden. Der Anschluss des Sensors nach dem 4-Klemmen-Konzept wird somit erforderlich. Dabei werden zwei getrennte Leiterschleifen über die beiden signalgebenden Elemente (z.B. Kontakte) geschlossen. Es sind für die sicherheitsgerichtete Einbindung des Sensors 4 Klemmen an der E/A-Peripherie erforderlich.

2 Eingänge + 2 Testausgänge

Querschluss-Sicherheit

Mit diesem Verfahren kann mit Standardbaugruppen eine vollständige Fehleraufdeckung auf den Sensor-Anschlussleitungen realisiert werden. Es ist keine besondere Verlegung der Anschlussleitungen erforderlich.

Sicherheitsgerichtete Hardware-Eingangssignale

Im Grundprinzip entspricht es dem 3-Klemmen-Konzept. Die erweiterten Maßnahmen haben zum Ziel, den reinen Querschluss (d.h. keine Verbindung zu M- oder P-Potenzial) zwischen zwei Leitungen aufzudecken.

Anwendungsbeispiel: Not-Halt

Merkmale

- Der Sensor wird von zwei Testausgängen der PLC mit je 24 V direkt angesteuert und über die beiden Eingangs-Kanäle 1 und 2 an die sicherheitsgerichtete Steuerung geführt.
- Der Testausgang 1 wird um tx gegenüber Testausgang 2 verzögert geschaltet. Dies ergibt als Erwartungshaltung einen eindeutigen Signalverlauf an den Eingangs-Kanälen 1/2.
- Eine 1-kanalige Testroutine in der PLC prüft diese Erwartungshaltung. Der Test kann im Rahmen der Zwangsdynamisierung durchgeführt werden.
- In Verbindung mit dem kreuzweisen Datenvergleich und der Zwangsdynamisierung können alle Fehler (P- und M-Kurzschluss) inkl. reinem Querschluss in den Anschlussleitungen aufgedeckt werden.

Anmerkung 1:

Das vorgestellte Konzept ist nur anwendbar beim Einsatz von kontaktbehafteten Sensoren mit geschlossenen Leiterschleifen (Ruhestromprinzip). Bei Elektroniksignalen muss die Leitungsüberwachung durch den Sensor sichergestellt werden.

Anmerkung 2:

Wenn kein Sicherheitsbauteil (z.B. Not-Halt-Taster) als Sensor eingesetzt wird, müssen die beiden signalgebenden Elemente (z.B. Schaltkontakte beim Taster) mechanisch entkoppelt sein.

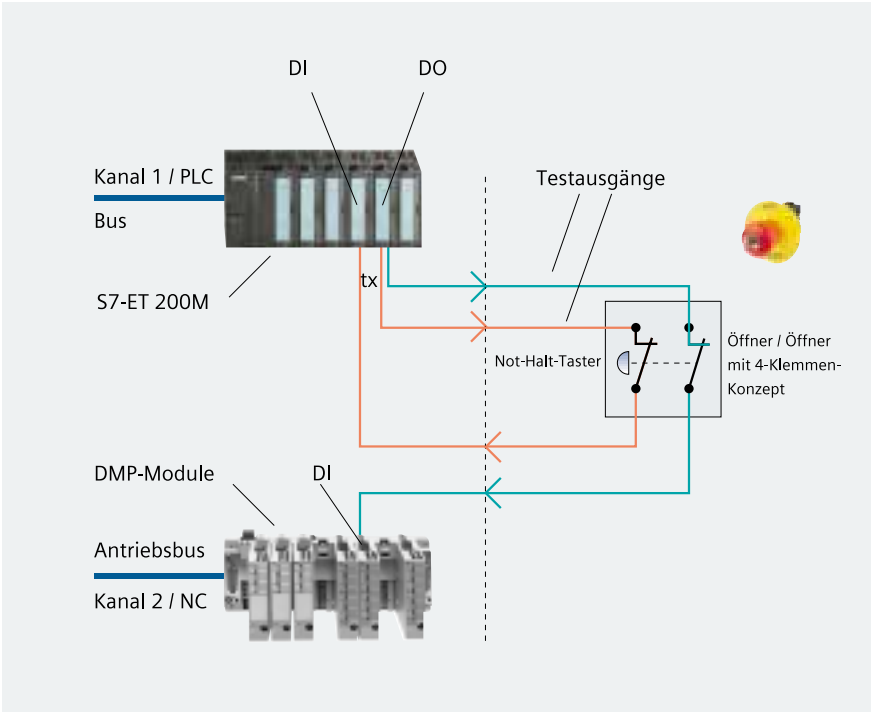


Bild 8/27
Sensor-Einbindung mit 4-Klemmenkonzept – Beispiel Not-Halt

Sicherheitsgerichtete Hardware-Ausgangssignale – P/P-schaltend

Bei P/P-schaltender Ausführung schalten immer zwei Aktoren in Reihe den Lastkreis. Beide Kanäle (NC und PLC) steuern die Aktoren mit Plus-Potential (24 V) an (Plus-Plus-schaltend). Als Aktoren können z.B. zum Schalten von Motoren handelsübliche Schütze mit zwangsgeführten Rückmeldekontakten eingesetzt werden.

Die Rückmeldung vom Lastkreis ist so direkt wie möglich von der Prozessgrösse abzuleiten. So ist z.B. die direkte Rückmeldung des Hydraulikdruckes über einen Druck-Sensor oder die Rückmeldung der bewegten Mechanik (Endanschlag) über einen Bero, der indirekten Rückmeldung des Hydraulikventils vorzuziehen.

Anwendungsbeispiel: 400V Lastspannug

- sichere Abschaltung der 400 V Lastspannung von Normasynchronmotoren
- sichere Abschaltung der 400 V Lastspannung von dezentralen Aggregaten

Merkmale

- Der Lastkreis wird immer 2-kanalig angesteuert
- Der Aktor ist doppelt vorhanden - die Last wird damit immer 2-kanalig unterbrochen bzw. geschaltet
- Als Aktoren können handelsübliche (Standard-)Bauteile wie z.B. Schütze, Ventile, usw. eingesetzt werden, da sie doppelt vorhanden sind.
- Die zwangsgeführten Rückmeldekontakte (Öffner) der Aktoren liegen fest auf 24 V, werden in Reihe geschaltet und von der PLC 1-kanalig zurückgelesen.
- In Verbindung mit der Zwangsdynamisierung können Fehler in der Ansteuerung und an beiden Aktoren aufgedeckt werden
- Beim Ausfall eines Aktors lässt sich die Last mit dem zweiten Kanal weiterhin abschalten
- Ein 1-kanaliges, prozessabhängiges Schalten des Aktors, aussschließlich über die PLC, ist möglich.

Sicherheitsgerichtete Hardware-Ausgangssignale – P/M-schaltend

Bei P/M-schaltender Ausführung schaltet nur ein einziger Aktor den Lastkreis. Der NC-Kanal steuert den Aktor mit Plus-Spannung (24 V) an, der PLC-Kanal steuert den Aktor mit Minus-Potential (0 V) (Plus-Minus-schaltend). Diese Variante der Ansteuerung ist immer dann erforderlich, wenn zur

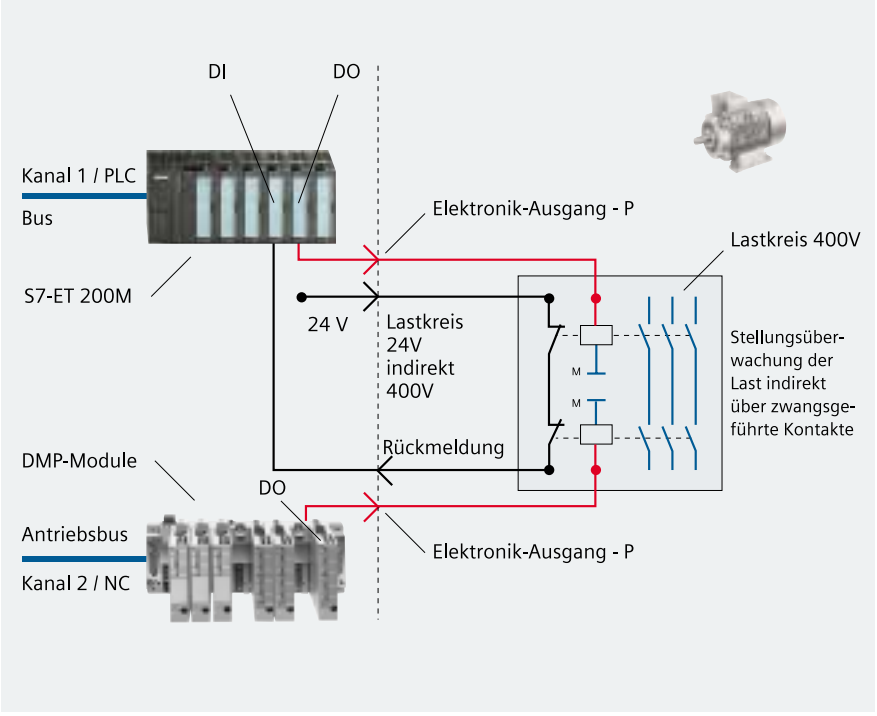


Bild 8/28
400 V-Lastkreis – P/P-schaltend – Beispiel Normasynchronmotor

direkten Ansteuerung des Lastkreises nur eine Magnetspule zur Verfügung steht. Das ist z.B. der Fall bei:

- Zuhaltemagneten an Schutztüren
- im Motor integrierten Haltebremsen
- über Ventile hydraulisch gesteuerten Betriebsbremsen (z.B. für Linearmotoren)

Die Rückmeldung vom Lastkreis ist so direkt wie möglich von der Prozessgrösse abzuleiten. So ist z.B. die direkte Rückmeldung des Hydraulikdruckes über einen Druck-Sensor oder die Rückmeldung der bewegten Mechanik (Endanschlag) über einen Bero, der indirekten Rückmeldung des Hydraulikventils vorzuziehen. Ist das Stellglied im Lastkreis wie hier nur einfach vorhanden, so sind weitere Maßnahmen wie z.B. zyklische Funktionstests des Stellgliedes erforderlich.

Anmerkung:

Steht kein Rückmeldekontakt zur Verfügung, so lässt sich grundsätzlich wie im Anwendungsbeispiel „Sichere Bremsenansteuerung – P/M-schaltend" beschrieben verfahren.

- In Verbindung mit der Zwangsdynamisierung können Fehler in der Ansteuerung und am Aktor aufgedeckt werden
- Fällt der Aktor aus, kann die Last über den spezifischen Pfad nicht mehr sicher abgeschaltet werden. In diesem Fall müssen, je nach Gefahrenanalyse und Ausführung des Aktors, zusätzliche Maßnahmen erfolgen, wie z.B. zentrale Abschaltung und erweiterte Testmaßnahmen.
- Ein 1-kanaliges, prozessabhängiges Schalten des Aktors, ausschließlich über die PLC, ist möglich.

Anwendungsbeispiel: Sichere Bremsenansteuerung – P/M-schaltend

Das Grundprinzip ist im Abschnitt „Sicherheitsgerichtete Hardware-Ausgangssignale – P/M-schaltend" beschrieben.

Die „sichere Bremsenansteuerung" ist Bestandteil der Funktion „sicheres Bremsenmanagement".

Beschreibung hierzu siehe „Absturzsicherung an Vertikalachsen".

Merkmale

- Der Lastkreis wird immer 2-kanalig angesteuert.
- Der Aktor Bremse ist nur einfach vorhanden. Die Prozessgröße, in diesem Fall das Bremsenmoment, wird nur 1-kanalig aufgebracht.
- Das Rückmeldesignal wird aus dem masseseitigen Anschluss der Magnetspule gebildet. Damit können M-Kurzschlüsse und P-Kurzschlüsse sicher aufgedeckt werden. Das 3-Klemmen-Konzept ist somit auch hier anwendbar.
- Der Elektronik-Ausgang - P wird um tx gegenüber dem Relais-Ausgang - M verzögert geschaltet. Dies ergibt als Erwartungshaltung einen eindeutigen Signalverlauf am Rückmeldeeingang.
- Eine 1-kanalige Testroutine in der PLC prüft diese Erwartungshaltung und kann im Rahmen der Zwangsdynamisierung durchgeführt werden.
- Als erweiterte Testmaßnahme wird ein sicherer Bremsentest vorgesehen, der das tatsächlich verfügbare Bremsmoment prüft. Diese Funktion steht mit dem „sicheren Bremsenmanagement" zur Verfügung. Die Überprüfung des Bremsmomentes wird in die Zwangsdynamisierung für den Teststop (Test der Abschaltpfade) eingebunden.
- Bei Spannungsausfall oder Leitungsbruch stellt sich der sichere Zustand der Bremse mechanisch über die Rückstellfedern automatisch ein.
- Als Aktoren können nur betriebsbewährte Bauteile nach EN 954-2 eingesetzt werden.

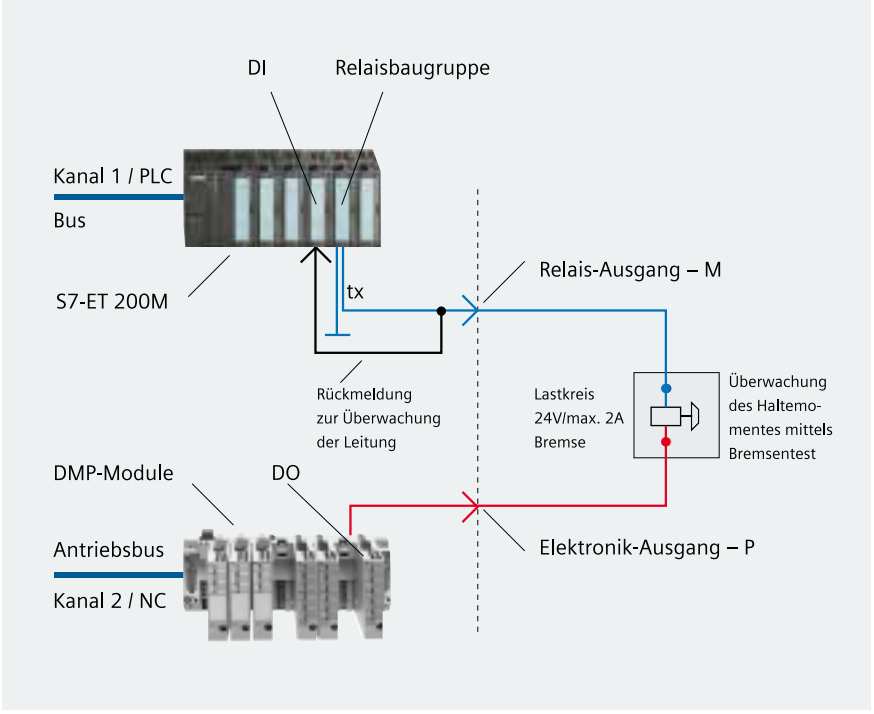


Bild 8/29
24 V-Lastkreis – P/M-schaltend – Beispiel sichere Bremsenansteuerung

Sicherheitsgerichtete Hardware-Ausgangssignale – P/M-schaltend mit Relais-Zwischenstufe

Bei diesem Beispiel wird, im Gegensatz zur vorher beschriebenen direkten P/M-schaltenden Version, der Lastkreis über eine zusätzliche Relais-Zwischenstufe zur Stromverstärkung angesteuert. Die Relais-Zwischenstufe kann bzw. muss dann eingesetzt werden, wenn keine 2 A-Ausgangs-Baugruppe der NC-Peripherie und / oder keine S7-Relais-Baugruppe zur Verfügung steht, oder wenn der zu schaltende Laststrom > 2 A ist.

Bei den in NC und PLC verwendeten Ausgängen handelt es sich um Standard-Ausgänge, mit denen die Relais-Zwischenstufe P/P-schaltend angesteuert wird.

Achtung!

Durch die Relais-Zwischenstufe wird, im Vergleich zum Best-Case (schneller, kontaktfreier NC-Pfad schaltet), die Reaktionszeit um die Schaltzeit des Relais verlängert. Dies führt zu längeren Reaktionszeiten und damit zu einem größeren Durchsackweg im Fehlerfall.

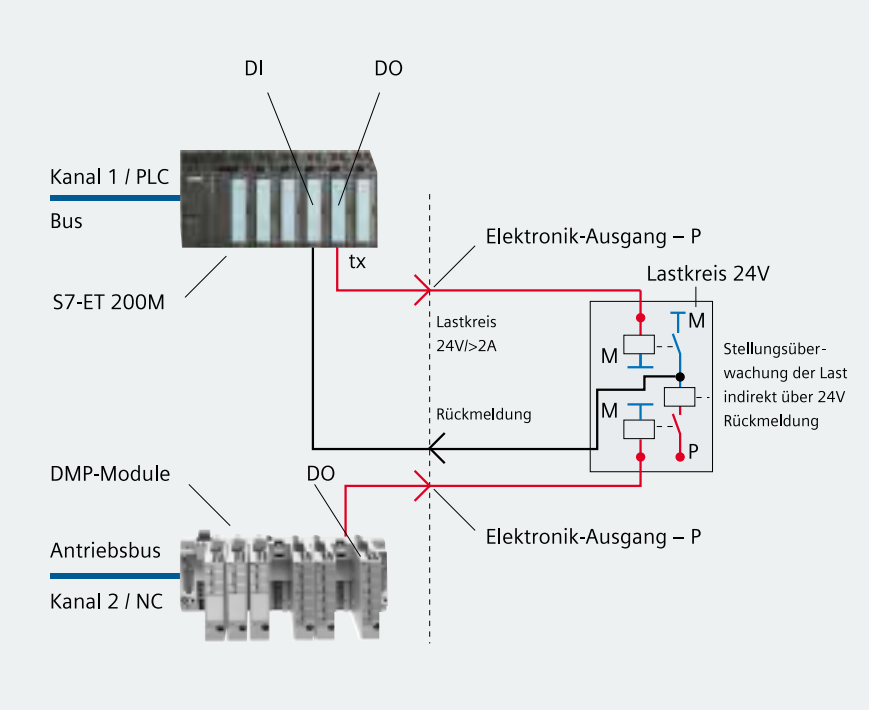


Bild 8/30
24 V-Lastkreis – P/M-schaltend mit Relais-Zwischenstufe für > 2 A

Anwendungsbeispiel: 24 V Lastspannung > 2 A

- Lastspannungsversorgung von de zentralen Einheiten mit > 2 A
- Bremsen mit > 2 A

Merkmale

- Prinzipiell gelten die gleichen Merkmale wie bei der direkten P/M-schaltenden Ansteuerung.
- Die Ansteuerung im 24 V-Lastkreis bleibt, wie schon in Bild 8/30: „24 V-Lastkreis – P/M-schaltend bis 2 A und bis 10A“ gezeigt, P/M-schaltend.
- Die Einbindung der zwangsgeführten Rückmeldekontakte der Relais-Zwischenstufe ist nicht zwingend erforderlich. Es können daher Standard-Relais ohne zwangsgeführte Rückmeldekontakte eingesetzt werden. Voraussetzung hierfür ist allerdings die Einbindung der direkten Rückmeldung vom M-Potenzial des Lastkreises.
- Fehlfunktionen im Pfad des Lastkreises werden durch die direkte Rückmeldung vom M-Potenzial aufgedeckt wie z.B.
  – Das nicht Schalten / Abfallen der Relais (z.B. durch Verkleben, Verhaken der Relaiskontakte)
  – Kurzschlüsse auf den 24 V-Ansteuerleitungen und des Lastkreises.

Sensor-/Aktor-Einbindung über die fehlersicheren Baugruppen von ET 200S PROFIsafe

Grundstruktur

Die Sensoren und Aktoren werden ohne externe Auswertegeräte direkt an die sicheren Eingänge und – Ausgänge der ET 200S PROFIsafe angeschlossen. Die Signale stehen dann über eine sichere Kommunikation mittels PROFIsafe der „SINUMERIK Safety Integrated"-Plattform zur Verfügung. Durch den Einsatz von ET 200S PROFIsafe vereinfacht sich die Sensor-/Aktor-Einbindung erheblich.

Sie ist:

- Einfacher in der Installation
- Modularer im Aufbau
- Flexibler in der Anwendung
- Übersichtlicher in der Dokumentation

Bild 8/31
Sensor-Aktor-Einbindung über ET 200S PROFIsafe

Merkmale

- Fehlersichere ET 200S Baugruppen für Eingänge F-DI, für Ausgänge F-DO und für Gruppenabschaltungen mit dem Powermodul PM-E F
- Sichere Kommunikation über PROFIBUS-DP mittels PROFIsafe Profil
- Einheitliches Aufbaukonzept, bei dem für Steuerungskategorie 3 sichere und nicht sichere Baugruppen gemischt werden können
- Motorstarter in sicherer Ausführung über das Powermodul PM-D F mit 6 Lastgruppen
- Projektierungstool Distributed Safety aus SIMATIC S7

Beispiel zur Sensor-/Aktor-Einbindung über die fehlersicheren Baugruppen der ET 200S PROFIsafe siehe Kapitel „Sensor-/Aktor-Einbindung".

Anwendungsbeispiele

- Einrichtbetrieb bei geöffneter Schutztür
  Bei geöffneter Schutztür können die Vorschub- oder Spindelantriebe mit sicher reduzierter Geschwindigkeit gefahren oder auf Stillstand sicher überwacht werden. Die Antriebe können zu jedem Zeitpunkt unter der Kontrolle der Elektronik bleiben und müssen nicht von der Energie getrennt werden. Mit den Funktionen zur Bereichserkennung und zur Verfahrbereichsabgrenzung lassen sich Arbeits- und Schutzbereiche in sicherer Technik realisieren. Der Einsatz eines Zustimmtasters ist, in Verbindung mit SINUMERIK Safety Integrated, nicht zwingend vorgeschrieben. Er kann jedoch, je nach Anforderung, z.B. zur Umschaltung von Sicherheitsfunktionen genutzt werden. Im Standardfall dürfen die Antriebe nur über Tipptasten im Totmannbetrieb* gefahren werden.

- Testbetrieb bei geöffneter Schutztür
  Erstmals ist auch ein Programm-Testbetrieb möglich, bei dem komplette Programme oder Programmteile mit sicher reduzierter Geschwindigkeit in einem „Trockenlauf" durchfahren werden können. Der Bediener hält dabei durch Betätigen einer Taste, meistens mit der Starttaste, den kontinuierlichen Ablauf des Programms aufrecht. Erkennt er beim Test einen Programmfehler, so kann er das Programm durch Loslassen der Starttaste oder durch Betätigen von Not-Halt anhalten. Die Sicherheitsfunktionen sind auch während dieser Testphase aktiv. Sie sprechen beim Verletzen der Grenzwerte an und setzen die Antriebe automatisch still.

- Integrierter, kontaktfreier Not-Halt
  Die Not-Halt-Taste kann direkt mit ihren beiden Kontakten, ohne weitere Auswertelogik, an die redundante Eingangsperipherie von PLC und NC angeschlossen werden oder an die fehlersicheren ET 200S PROFIsafe Eingabebaugruppen. Die logische Verknüpfung und die erforderlichen Reaktionen erfolgen intern in sicherer Technik. Die elektrischen Antriebe werden sicher stillgesetzt und anschließend über die Elektronik kontaktfrei von der Energie getrennt. Ein Wiederanlauf wird sicher verhindert. Externe Energien, wie z.B. Hydraulik oder Laser usw., können über die redundante oder fehlersichere Ausgangsperipherie von der integrierten Not-Halt-Logik und nachgeschalteten Aktoren (Leistungsschütze, Ventile, ...) in sicherer Technik abgeschaltet werden.

Zertifizierung

Eine Zertifizierung der beschriebenen Safety Integrated Funktionen gemäß DIN V VDE 0801, EN 954-1 und EN 60204 liegt seit 1996 vor.

Eine Zertifizierung der beschriebenen Safety Integrated Funktionen nach EN 954-1 (Kategorie 3) und IEC 61508 (SIL 2) sowie eine NRTL-Listung liegt vor.

* Totmannbetrieb

Der Begriff kommt ursprünglich aus der Bahntechnik.

Bedeutung: Die Funktion bleibt nur so lange erhalten, wie das Betätigungselement (Tipptaste) gedrückt ist. Nach dem Loslassen des Betätigungselements wird die Funktion unterbrochen und ein Stillsetzen der gefahrbringenden Bewegung eingeleitet.

8.2 Safety Unit

Das Sicherheitspaket für Umformtechnik

An allen Produktionsmaschinen, insbesondere an Pressen, sind zum Schutz des Bedienpersonals Vorkehrungen zu schaffen, die eine Gefährdung im Bearbeitungsprozess ausschließen. Dies kann durch Absicherung der Maschinen über Schutztüren oder durch Lichtgitter geschehen. Muss während des Fertigungsprozesses allerdings häufiger betriebsmäßig durch den Bediener eingegriffen werden, sind die Maschinenreaktionen, z.B. durch Geschwindigkeitsüberwachungen, zu kontrollieren, um bei fehlerbedingten Ausfällen an Steuerung und Mechanik eine gefahrbringende Bewegung der Maschinen zu vermeiden.

Um solche Anforderungen abdecken zu können, wurde die Safety Unit TM 121 entwickelt.

Sie ist so konzipiert, dass folgende Sicherheitsanforderungen erfüllt werden:

- EN 954-1 sicherheitsbezogenen Teile von Steuerungen.
  Hier wird die Kategorie 4 eingehalten.
- IEC 61508 Functional Safety of electrical/electronic/programmable safety-related systems
  SIL 3 wird hierbei erfüllt.
- EN 61496 Sicherheit von Maschinen, berührungslos wirkenden Schutzeinrichtungen

Bild 8/32
Safety Unit TM 121C

Redundantes (zweikanaliges) elektronisches Prozessorsystem mit:

32 sicherheitsgerichteten Eingängen, 24 V
8 sicherheitsgerichteten Ausgängen, 24 V, 2 A
8 Standardausgängen, 24 V, 0.5 A
2 sichere Frequenzeingänge, 24 V, 500 Hz

Versorgung:
24V DC

mech. Festigkeit:
Erfüllung eines höheren Schärfegrades bei mechanischer Belastung gemäß EN 61496

Bild 8/33
Safety Unit – Technische Daten

Berücksichtigt sind Auszüge davon, d.h. höhere Schärfegrade z.B. bei mechanischer Belastung oder EMV.

Damit sind europaweit die Voraussetzungen zur Realisierung von Sicherheitsaufgaben an Maschinen einschließlich handbedienter Pressen erfüllt.

In der Steuerung fest hinterlegt sind Standardbausteine, wie sie zur Absicherung an allen Arten von Maschinen benötigt werden. Genannt seien hier Schutzgitter- bzw. Schutztürüberwachungen oder auch Notauskreise. Zusätzliche wurden spezielle Ausprägungen realisiert, die an bestimmten Maschinenarten, wie **mechanische**, **hydraulische Pressen** oder **Abkantpressen**, vorkommen.

Diese Bausteine werden über ein mitgeliefertes Parametriertool verschaltet.

Beispiel:
Funktionsbausteine für mechanische Pressen

- 2-Hand-Bedienung
- Nockeneingänge sicher (Hochlauf, Nachlauf, Übernahme)
- Betriebsartenauswahl
- Not-Halt („spannungsfrei schalten"), Einrücksperre
- Ansteuerung Kupplungs-Bremskombination (mit Überwachung)
- Schutztür / Schutzgitter / Lichtvorhang
- Laufwächterkontrolle (über Frequenzeingang)

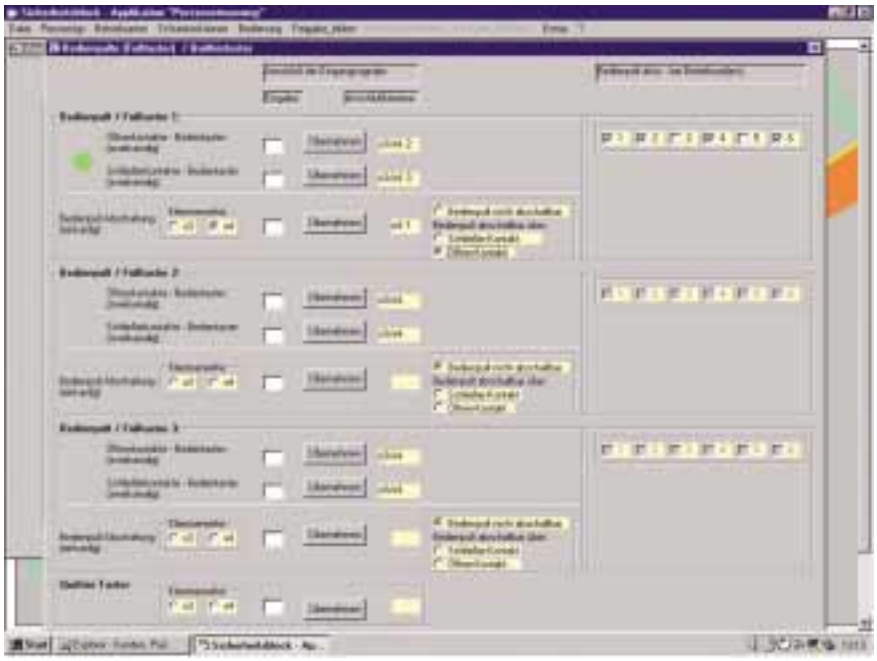


Bild 8/34
Beispielmaske der Parametriersoftware

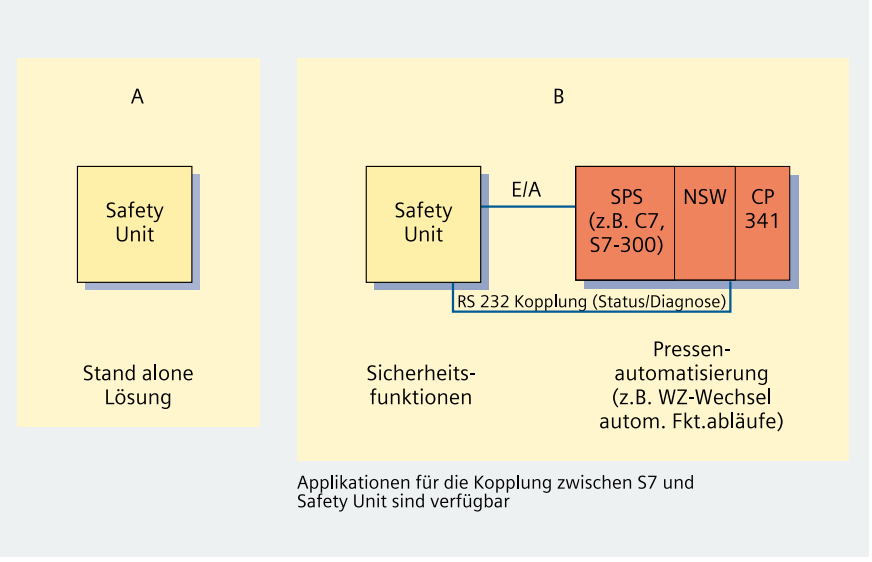


Bild 8/35
Safety Unit – Topologie

8.3 Safety Integrated für Motion Control Systeme

Unser Dienstleistungsangebot

Übersicht

Komplettiert wird das Angebot der Safety Integrated-Produkte durch ein umfangreiches Dienstleistungspaket. Das Leistungsspektrum für Maschinenhersteller und Maschinenbetreiber umfasst:

- **Konzepterstellung**
  Ausgehend von der Gefahrenanalyse und der gewünschten Bedienphilosophie wird gemeinsam mit dem Kunden eine entsprechende Adaption der Sicherheitsfunktionen für die Maschine erarbeitet.

- **Hardware-Projektierung**
  Integration und Einarbeitung des Sicherheitskonzeptes in die Schaltpläne. Dabei werden sicherheitsgerichtete Sensoren und Aktoren ausgewählt und deren Verdrahtung definiert.

- **SPL-Projektierung**
  Für die sichere programmierbare Logik (SPL) werden alle notwendigen Module und Objekte erstellt und diese in das Gesamtsystem eingebunden.

- **Inbetriebnahme**
  Ausgehend von den erstellten Projektierungen werden die Sicherheitsfunktionen in Betrieb genommen. Dazu stellt der Kunde die Maschine so zur Verfügung, dass die Antriebe verfahren werden können und der Schaltschrank entsprechend der Projektierung verdrahtet ist.

- **Abnahmetest mit abschließendem Abnahmeprotokoll**
  Alle Sicherheitsfunktionen werden entsprechend den Anforderungen geprüft. Die Prüfergebnisse und die dabei entstandenen Messdiagramme werden in einem Abnahmeprotokoll festgehalten. Dieses ist sowohl für den Maschinenhersteller als auch für den -betreiber ein eindeutiger Qualitätsnachweis der funktionalen Sicherheit der Maschine.

- **Workshop**
  Workshops zum Thema Maschinensicherheit werden kundenspezifisch angepasst und, wenn gewünscht, beim Kunden durchgeführt.

- **Hotline**
  Bei aktuellen Störungen oder bei Problemen während der Inbetriebnahme sind unter der Hotline 0180/50 50 222 Experten zum Thema Safety Integrated erreichbar.

- **Support Anfrage**
  Sie können sich direkt an die Techniker wenden, in dem Sie über das Internet eine Support-Anfrage senden.

www.siemens.de/automation/support-request

- **Vor-Ort-Service**
  Experten analysieren vor Ort Störungen. Die Ursachen werden beseitigt bzw. ein Lösungskonzept wird erarbeitet und bei Bedarf umgesetzt.

Nutzen

- **Zeitersparnis**
  bei der Konzepterstellung bis hin zur Abnahme der Sicherheitsfunktion.
- **Schnelle und kompetente Hilfe**
  bei Problemen während der Inbetriebnahme und bei Maschinenstörungen.
- **Schnelle Erweiterung des eigenen Know How**
  durch den effektiven Know How Transfer unserer sicherheitstechnischen Lösungen.

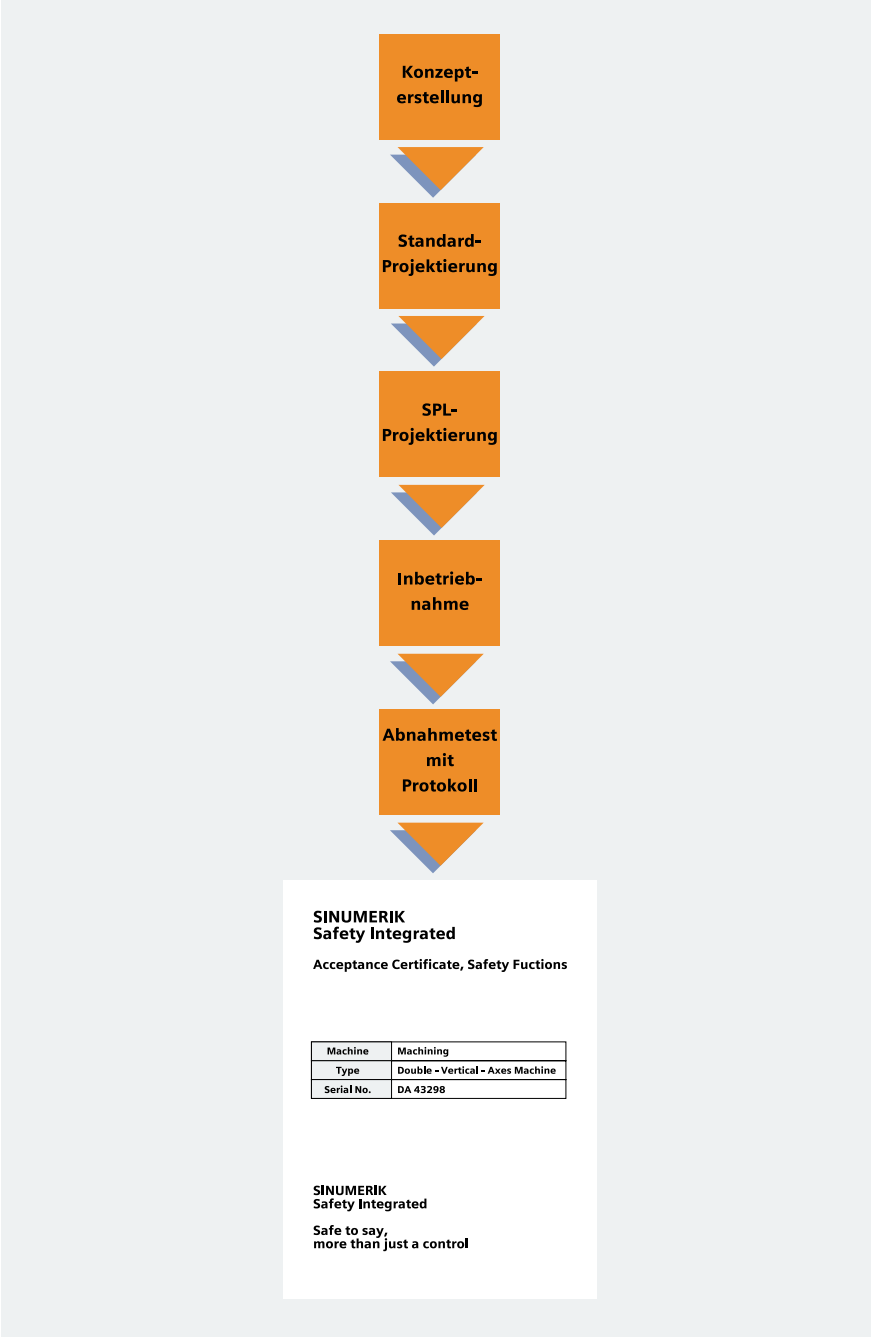
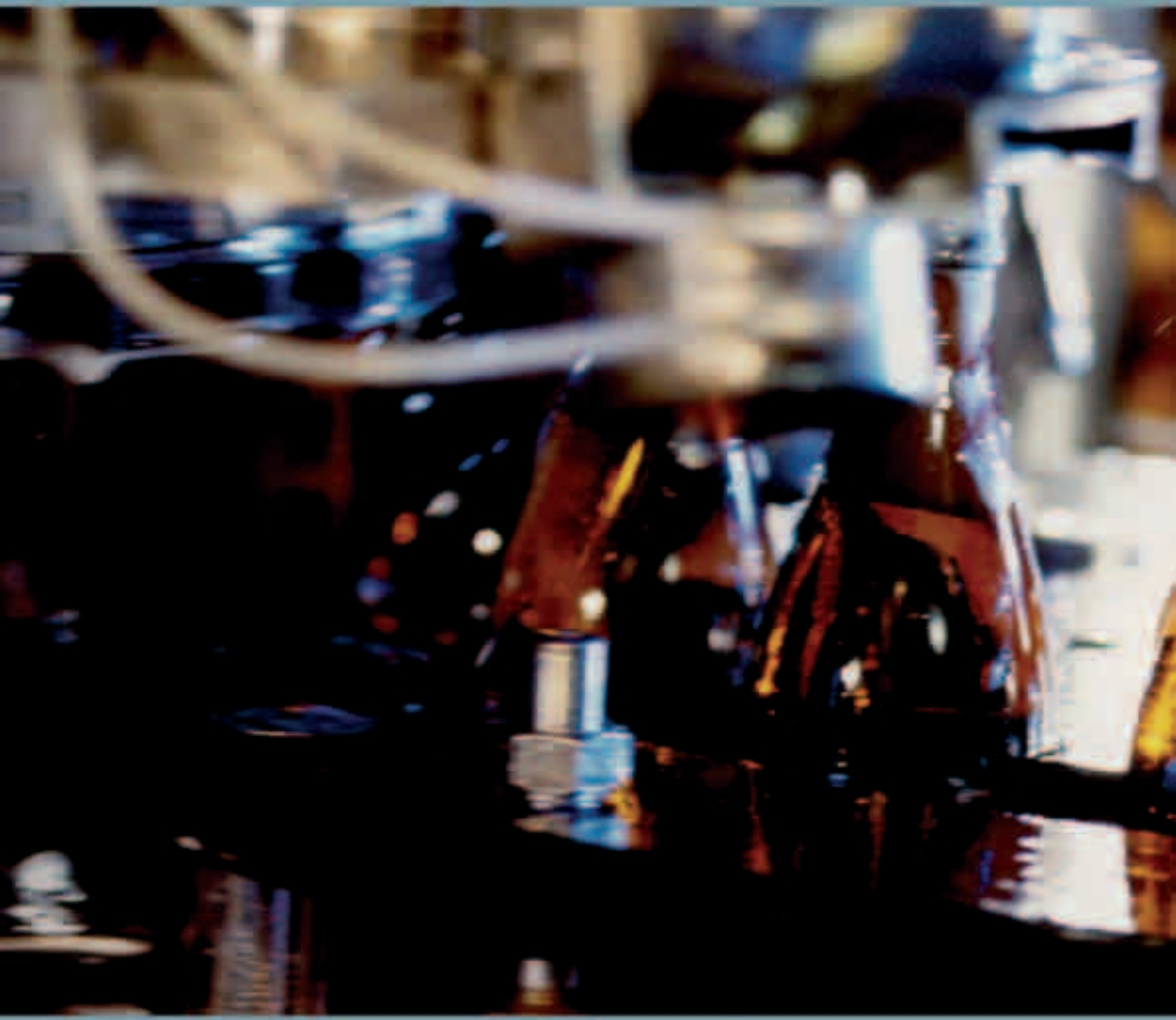


Bild 8/36
Ablaufplan unseres Dienstleistungsangebotes



9.1 MASTERDRIVES und SIMODRIVE 611universal

9.2 SINAMICS Safety Integrated

9.3 Frequenzumrichter SIMATIC ET 200S FC

Fehlersichere Antriebe

9

sinamics

9 Fehlersichere Antriebe

9.1 MASTERDRIVES und SIMODRIVE 611 universal

Übersicht

Maßnahmen zum Einrichten bei geöffneten trennenden Schutzeinrichtungen sind nach den meisten europäischen Produktnormen für Maschinen vorgesehen. Die Mindestanforderung für Antriebe ist die Vermeidung von unerwartetem Anlauf.

Die Antriebssysteme SIMOVERT MASTERDRIVES und SIMODRIVE 611 universal unterstützen diese Forderung mit der Funktion „sicherer Halt". Die Funktion ist durch eine Baumusterprüfung von der Berufsgenossenschaft in Kategorie 3 nach EN 954-1 zertifiziert. Damit lassen sich wesentliche Anforderungen aus der EG-Maschinenrichtlinie einfach und wirtschaftlich umsetzen.

Bild 9/1
SIMOVERT MASTERDRIVES Kompakt-PLUS

Nutzen

- **Reduzierte Kosten:**
  Heute oft noch gebräuchliche motorseitige Schütze können entfallen. Der Projektierungs- und Verdrahtungsaufwand reduziert sich bei gleichzeitigem Platzgewinn im Schaltschrank.
- **Einfache Umsetzung:**
  Mittels definierter, externer Beschaltung (z.B. Sicherheitsschaltgerät) und integriertem Sicherheitsrelais kann die Funktion „sicherer Halt" als Applikation einfach realisiert werden.
- **Vereinfachte Maschinen-Abnahme:**
  Die Schaltungsprinzipien sind zertifiziert und bereits vielfach in der Praxis eingesetzt. Dadurch vereinfacht sich die Abnahme von Maschinen und Anlagen durch die entsprechenden Prüfinstitute.

Anwendungsbereich

Aufgrund ihrer kompakten und modularen Bauweise bieten die Gerätereihen SIMOVERT MASTERDRIVES und SIMODRIVE 611 universal leistungsfähige und zugleich wirtschaftliche Antriebslösungen, passend für viele Anwendungen z.B. im Bereich von Druck und Papiermaschinen, Verpackungsmaschinen, Textilmaschinen, Kunststoffmaschinen, Maschinen der Umformtechnik oder Bearbeitungsmaschinen für Holz, Glas und Stein.

Der „sichere Halt" dient in Verbindung mit einer Maschinenfunktion oder im Fehlerfall zum internen sicheren Abtrennen der Energiezufuhr zum Motor. Auch beim Stillsetzen über Not-Halt gemäß Stop-Kategorie 0 oder 1 (nach EN 60204-1) kann der „sichere Halt" eingesetzt werden.

Aufbau

Der „sichere Halt" wird als Applikation realisiert. Basis ist die sichere Sperrung der Ansteuerimpulse der Leistungstransistoren im Antrieb. Eine definierte, externe Beschaltung sorgt über Klemmen für eine sichere Ansteuerung des im Antrieb integrierten Sicherheitsrelais. Das Sicherheitsrelais unterbricht die Stromversorgung für die Impulsübertragung im Leistungsteil. Über zwangsgeführte Kontakte kann der Schaltzustand des Relais extern ausgewertet werden.

Bild 9/2
SIMODRIVE 611 universal

Funktion Sicherer Halt (SH)

Mit der Funktion „sicherer Halt“ werden die Impulse des Antriebes gelöscht und die Energiezufuhr zum Motor getrennt. Der Antrieb ist sicher drehmomentfrei. Über einen Rückmeldekontakt wird sein Schaltzustand angezeigt und kann somit überwacht werden.

Technische Daten

SIMOVERT MASTERDRIVES / SIMODRIVE 611universal	
Sicherheitsfunktion	• Sicherer Halt
Erreichbare Sicherheitsklassen	bis Kategorie 3 nach EN 954-1
Schutzart	IP20
Regelungsvarianten	• Servoregelung • Vektorregelung (nur MASTERDRIVES) • U/f-Steuerung (nur MASTERDRIVES)
Weitere Features	• Technologiefunktionen • Positionieren • Freie Funktionsbausteine (nur MASTERDRIVES)

9.2 SINAMICS Safety Integrated

Antriebsautarke, integrierte Sicherheitsfunktionen

Übersicht

Das Antriebssystem SINAMICS S120 unterstützt die Forderung „Vermeidung von unerwarteten Wiederanlauf“ mit integrierten Sicherheitsfunktionen. Neben dem „sicheren Halt“ ist auch erstmals eine „sichere Bremsenansteuerung“ integriert. Diese Funktionen sind durch eine Baumusterprüfung von der Berufsgenossenschaft nach Kategorie 3 (EN 954-1) und SIL 2 (IEC 61508) zertifiziert. Damit lassen sich wesentliche Anforderungen aus der EG-Maschinenrichtlinie einfach und wirtschaftlich umsetzen.

Bild 9/3
SINAMICS S120

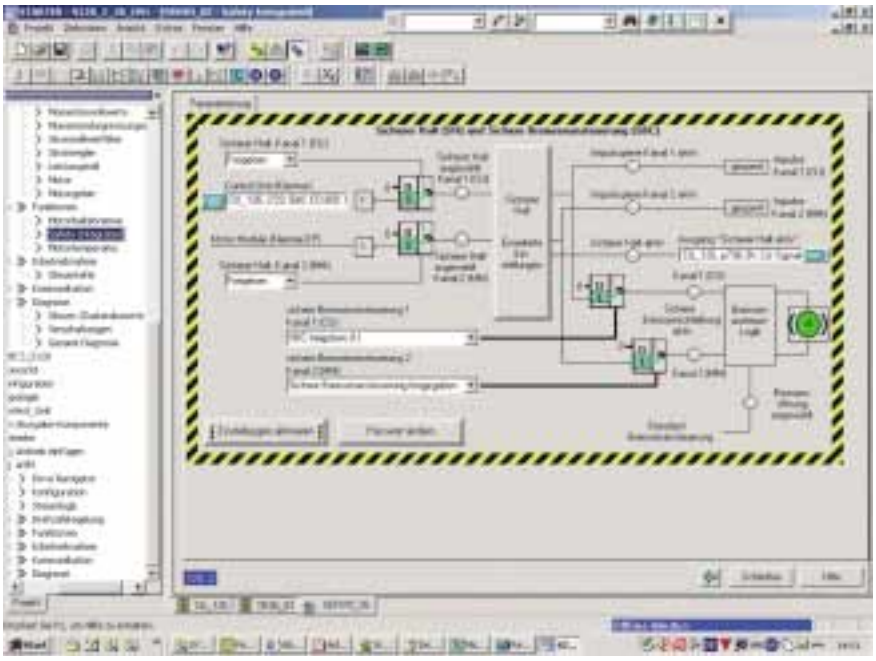


Bild 9/4
Projektierung der Sicherheitsfunktion

Alle Sicherheitsfunktionen werden bei Projektierung, Inbetriebnahme und Diagnose durch die Engineering-Software „Starter“ unterstützt.

Nutzen

- **Reduzierte Kosten:**
  In vielen Fällen lassen sich externe Schaltgeräte einsparen. Die Integration der Sicherheitstechnik ermöglicht praxisgerechte Sicherheitskonzepte bei gleichzeitiger Vereinfachung der Installationstechnik. Zusätzlich ergibt sich ein Platzgewinn im Schaltschrank.

- **Höhere Zuverlässigkeit:**
  Durch die konsequente elektronische Ausführung entfallen die früher verwendeten kontaktbehafteten integrierten Bauteile wie z.B. integriertes Sicherheitsrelais und Netzschütz.

- **Vereinfachte Maschinen-Abnahme:**
  Durch zertifizierte, integrierte Sicherheitsfunktionen vereinfacht sich die Abnahme von Maschinen und Anlagen durch die entsprechenden Prüfinstitute.

Anwendungsbereich

Aufgrund seiner innovativen Eigenschaften ist der SINAMICS S120 prädestiniert als das Antriebssystem in Produktionsmaschinen aller Art wie z.B. Druck und Papiermaschinen, Verpackungsmaschinen, Textilmaschinen, Kunststoffmaschinen, Maschinen der Umformtechnik oder Bearbeitungsmaschinen für Holz, Glas und Stein.

Bei den Anwendungen sind die integrierten Sicherheitsfunktionen die Grundlage zur Realisierung von praxisgerechten Sicherheitskonzepten an Maschinen und Anlagen.

Aufbau

Die Sicherheitsfunktionen sind im Antriebssystem komplett integriert und verfügen über antriebsspezifische Schnittstellen:

- 2 Eingangsklemmen für den „sicheren Halt“
- 2 Ausgangsklemmen für die „sichere Bremsenansteuerung“

Sie sind in sicherer Technik, voll elektronisch ausgeführt und bieten dadurch kurze Reaktionszeiten. Integrierte Selbsttests dienen der Fehleraufdeckung.

Funktionen

- **Sicherer Halt (SH)**
  Der „sichere Halt“ unterbricht direkt die Stromversorgung für die Impulsübertragung im Leistungsteil. Der Antrieb ist dadurch sicher drehmomentfrei. Eine Rückmeldung ist nicht erforderlich, sie kann jedoch über einen Ausgang oder per Software projektiert werden. Ein übergeordnetes Hauptschütz braucht zur Realisierung der Funktion „sicherer Halt“ nicht mehr vorgesehen werden.

- **Sichere Bremsenansteuerung (SBC)**
  Die Bremse wird zweikanalig, P/M-schaltend (Plus/Minus) angesteuert. Die Ansteuerleitungen werden bei An- bzw. Abwahl der Motorbremse überwacht.

Die Steuerleitungen für die Bremsenansteuerung können direkt mit der Motorleitung am Leistungsteil angeschlossen werden. Die Stromaufnahme der Bremse darf bis zu 2 A betragen.

Die Funktionen wirken antriebs- oder gruppenspezifisch wodurch ein oder mehrere Sicherheitskreis(e) zugeordnet werden können. Damit kann die Anlagenverfügbarkeit gesteigert werden.

Die Bremse bleibt bei **einem** Fehler in der Ansteuerung voll funktionsfähig!

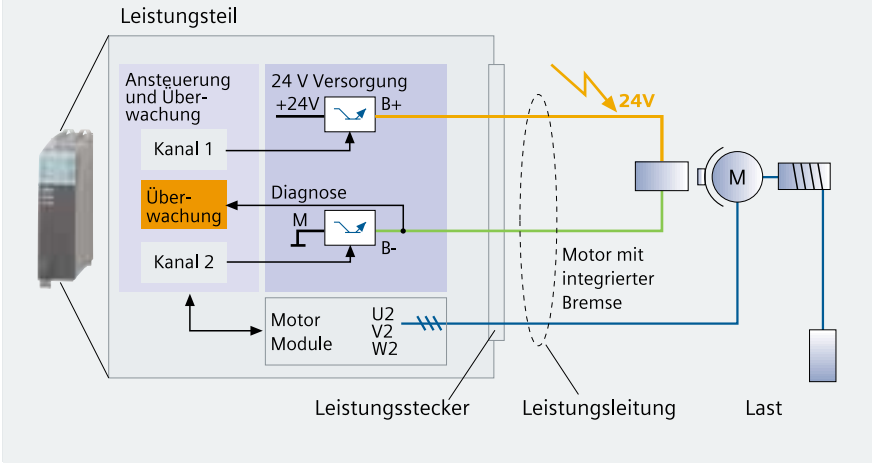


Bild 9/5
Sichere Bremsenansteuerung

Technische Daten

SINAMICS S120	
Erreichbare Sicherheitsklassen	• Bis Kategorie 3 nach EN 954-1 • Bis SIL 2 nach IEC 61508
Sicherheitskenngrößen	Kenngrößen (PFD-/PFH-Werte) nicht komponenten- sondern systemabhängig (Werte und Berechnung in zugehöriger Produktdokumentation)
Sicherheitsfunktionen	• Sicherer Halt • Sichere Bremsenansteuerung
Schutzart	IP20
Weitere Features	• Modularer Aufbau • Elektronische Typenschilder • Servoregelung • Vektorregelung • U/f-Steuerung

9.3 Frequenzumrichter SIMATIC ET 200S FC

Übersicht

Der Frequenzumrichter ergänzt das dezentrale Peripheriesystem SIMATIC ET 200S. Die SIMATIC ET 200S wird feinmodular aufgebaut aus Komponenten mit dezentraler Intelligenz, Ein- und Ausgängen, Motorstartern und Sicherheitstechnik. Der Umrichter, Typenbezeichnung SIMATIC ET 200S FC, regelt stufenlos die Drehzahl von Asynchronmotoren und löst Antriebsaufgaben mit einfacher Frequenzsteuerung bis hin zu anspruchsvoller Vektorregelung.

Der Frequenzumrichter ET 200S FC wird in einer Standard-Variante und in fehlersicherer Ausführung angeboten. Der fehlersichere Frequenzumrichter bietet neben dem „sicheren Halt" die integrierten Sicherheitsfunktionen „sicher reduzierte Geschwindigkeit" und „sichere Bremsrampe", die erstmalig auch in Verbindung mit geberlosen Normasynchronmotoren eingesetzt werden können. Alle Sicherheitsfunktionen sind gemäß Kategorie 3 nach EN 954-1 und SIL 2 nach IEC 61508 zertifiziert.

Bild 9/6
ET200S Station mit Ein-/Ausgängen, Motorstartern und Frequenzumrichtern ET 200S FC

Bild 9/7
Frequenzumrichter ET200S FC Failsafe in Baugröße B 82,2 kW oder 4,0 kW)

Der Frequenzumrichter ET 200S FC wird mit dem „Starter", einem maskenorientierten Engineering-Tool, in Betrieb genommen. Der „Starter" unterstützt auch die Inbetriebnahme und Diagnose der integrierten Sicherheitsfunktionen.

Nutzen

- **Flexible Lösung**
  Innerhalb einer ET 200S Station können fehlersichere und Standard-Komponenten gemeinsam betrieben werden. Das gilt auch den Frequenzumrichter. Flexible und einfach zu projektierende Lösungen mit geringem Aufwand an Hardwarefür die unterschiedlichsten Aufgaben werden so möglich.

- **Reduzierte Kosten**
  In vielen Fällen lassen sich externe Schaltgeräte durch Verwendung des „sicheren Halts“ einsparen. Die Integration der Sicherheitstechnik ermöglicht praxisgerechte Sicherheitskonzepte bei gleichzeitiger Vereinfachung der Installationstechnik. Zusätzlich ergibt sich ein Platzgewinn im Schaltschrank.

  Bisher einzigartig ist, dass sowohl die Funktion "sichere Bremsrampe" als auch die Funktion "sicher reduzierte Geschwindigkeit" ohne Motorgeber oder Encoder auskommen und mit minimalem Aufwand realisiert werden können.

- **Höhere Zuverlässigkeit**
  Der „sichere Halt“ ist rein elektronisch und kontaktfrei ausgeführt und sorgt so für kürzeste und zuverlässige Reaktionszeiten.

- **Vereinfachte Maschinenabnahme**
  Durch zertifizierte, integrierte Sicherheitsfunktionen vereinfacht sich die Abnahme von Maschinen und Anlagen durch die entsprechenden Prüfbehörden

Anwendungsbereich

- Neben einfachen Antriebsaufgaben, beispielsweise Förderapplikationen, unterstützt der Umrichter auch Anwendungen wie Wickel- und Abwickelantriebe und Hubwerke. Mit einem Motorgeber reicht die Skala bis hin zur präzisen Drehzahl- und Momentenregelung.

- Der Frequenzumrichter ET 200S FC kann generatorische Energie ins Versorgungsnetz zurückspeisen. Damit vereinfachen sich Applikationen mit dauerhaftem generatorischen Betrieb deutlich. Beispiele hierfür sind Abwickler, Absenken von Lasten in Hebezeugen oder elektrisches Bremsen größerer Schwungmassen.

- Die Funktion „sichere Bremsrampe“ ermöglicht ein sicher überwachtes Stillsetzen des Antriebs, auch mit geberlosen Asynchronmotoren. Nach dem Stillsetzen des Antriebs wird durch den „sicheren Halt“ ein Wiederanlaufen des Antriebs verhindert.

- Die „sicher reduzierte Geschwindigkeit“ erlaubt das langsame Verfahren eines Antriebs in Gefahrenbereichen, beispielsweise zum Einrichten oder zur Materialbestückung. Auch diese Funktion kann ohne Motorgeber mit Normasynchronmotoren realisiert werden.

Anmerkung:

Die Funktionen „sichere Bremsrampe“ und „sicher reduzierte Geschwindigkeit“ des Frequenzumrichters SIMATIC ET 200S FC dürfen nicht bei durchziehenden Lasten eingesetzt werden.

Aufbau

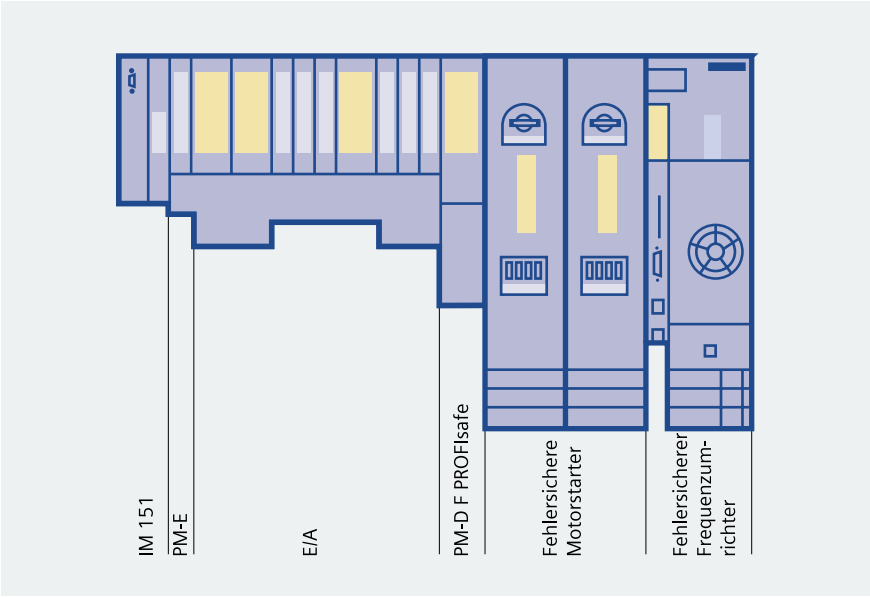


Bild 9/8
ET 200S-Station mit IM 151, fehlersicheren und Standard-Ein-/Ausgängen, fehlersicherem Motorstarter und Frequenzumrichter

Der fehlersichere Frequenzumrichter ET 200S FC besteht aus folgenden Komponenten:

- Regelungsbaugruppe ICU24F
- Leistungsteil IPM25 (lieferbar in zwei Baugrößen mit Leistungen von 0,75 kW, 2,2 kW und 4,0 kW)
- Terminalmodule zum Anschluss der Verdrahtung und zur Aufnahme von Regelungsbaugruppe und Leistungsteil

Nach dem Stecken der Baugruppen sind Regelungsteil und Leistungsteil des Frequenzumrichters miteinander verbunden.

Funktionen

- **Sicherer Halt (SH):** Der „sichere Halt" unterbricht die Stromversorgung für die Impulsübertragung im Leistungsteil und löscht zusätzlich die Impulse. Der Antrieb ist dadurch sicher drehmomentfrei und gegen Wiederanlauf geschützt.

  Zusätzlich erfolgt beim Abschalten über die einzelnen Abschaltpfade eine Prozessdynamisierung durch Überprüfung der Erwartungshaltung, die aus der jeweiligen Schaltaktion resultiert.

- **Sichere Bremsrampe (SBR):** Überwacht das Stillsetzen des Antriebs. Der Antrieb wird an einer einstellbaren Rampe abgebremst. Während des Stillsetzvorgangs wird laufend überwacht, ob die aktuelle Drehzahl der vorgegebenen Rampenfunktion folgt. Nach Unterschreiten einer (parametrierbaren) Mindestdrehzahl wird dann der „sichere Halt" aktiviert.

  Bei Versagen der Bremsfunktion wird der „sichere Halt" sofort ausgelöst und der Antrieb geht in den Fehlerzustand.

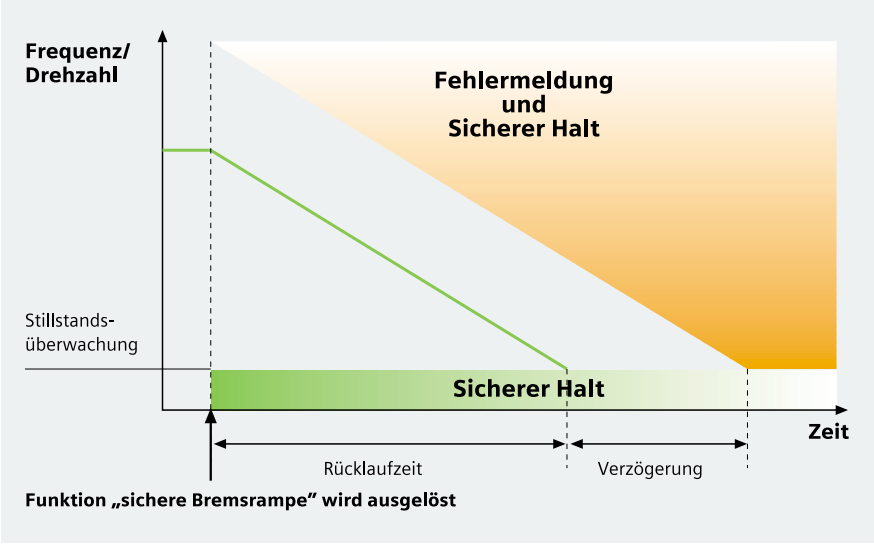


Bild 9/9
Sichere Bremsrampe des Frequenzumrichters SIMATIC ET 200S FC

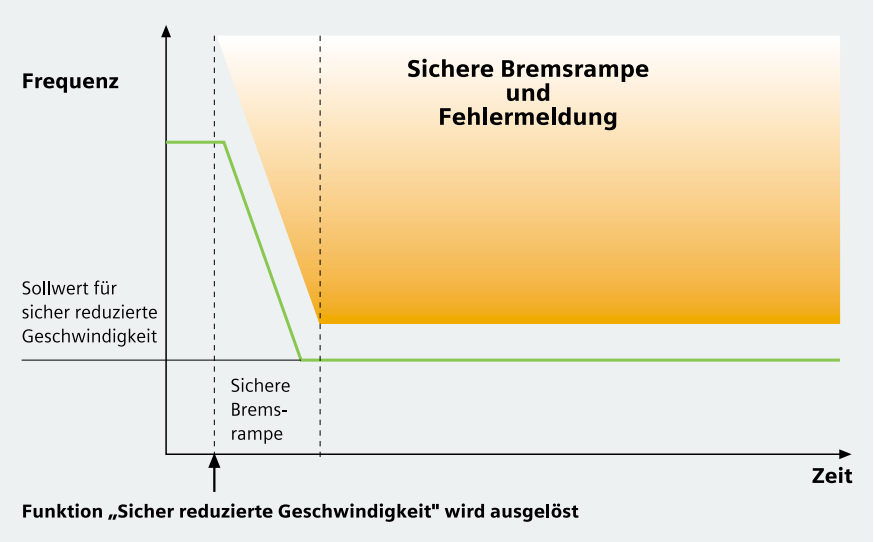


Bild 9/10
Sicher reduzierte Geschwindigkeit des Frequenzumrichters SIMATIC ET 200S FC

- **Sicher reduzierte Geschwindigkeit (SG):** Überwacht die Drehzahl auf einen oberen Grenzwert.

  Ist beim Einleiten der „sicher reduzierten Geschwindigkeit" die Drehzahl größer als der sichere Grenzwert, so wird die Drehzahl des Antriebs zunächst mit der „sicheren Bremsrampe" reduziert, wobei als Zieldrehzahl nicht Drehzahl Null sondern der sichere Geschwindigkeitsgrenzwert gesetzt wird.

  Ist beim Einleiten der „sicher reduzierten Geschwindigkeit" die Drehzahl kleiner als der sichere Grenzwert, wird die Überwachung auf den reduzierten Geschwindigkeitsgrenzwert sofort aktiv.

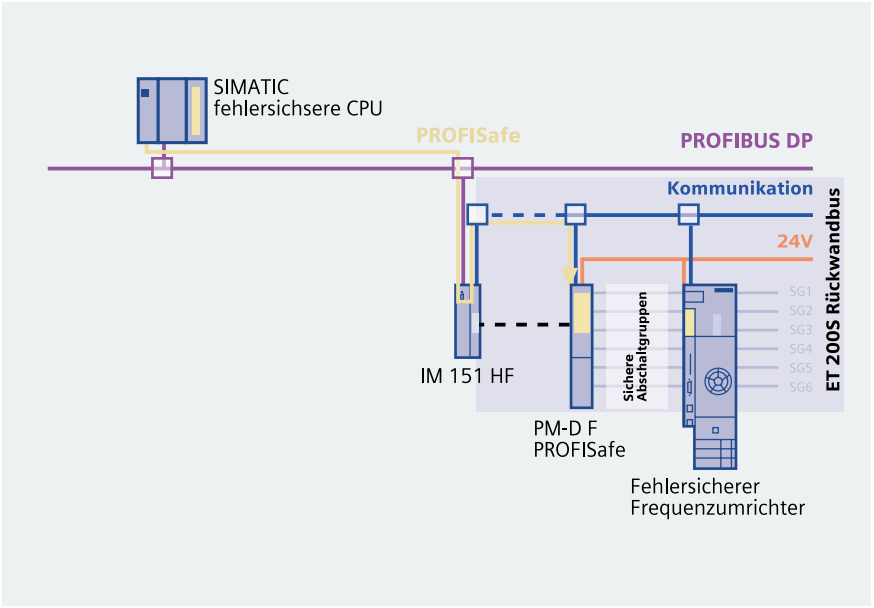
  Beim Ansprechen der Überwachung wird der Antrieb mit der „sicheren Bremsrampe" angehalten. Der Frequenzumrichter geht anschließend in den Fehlerzustand.

Integration

Der Frequenzumrichter ET 200S FC ist vollständig in das System ET 200S integriert und verzichtet daher auf eigene Ein- und Ausgänge. Die Ansteuerung der fehlersicheren Funktionen des Umrichters erfolgt innerhalb der ET 200S über Signale im Rückwandbus, genauer über sichere Abschaltgruppen eines Powermoduls PM-D F. Der Umrichter wertet zwei dieser Abschaltgruppen über sichere Eingänge aus.

Die SIMATIC ET 200S stellt drei grundsätzliche Möglichkeiten für die Konfiguration fehlersicherer Anlagen und damit für die Ansteuerung der fehlersicheren Umrichterfunktionen zur Verfügung.

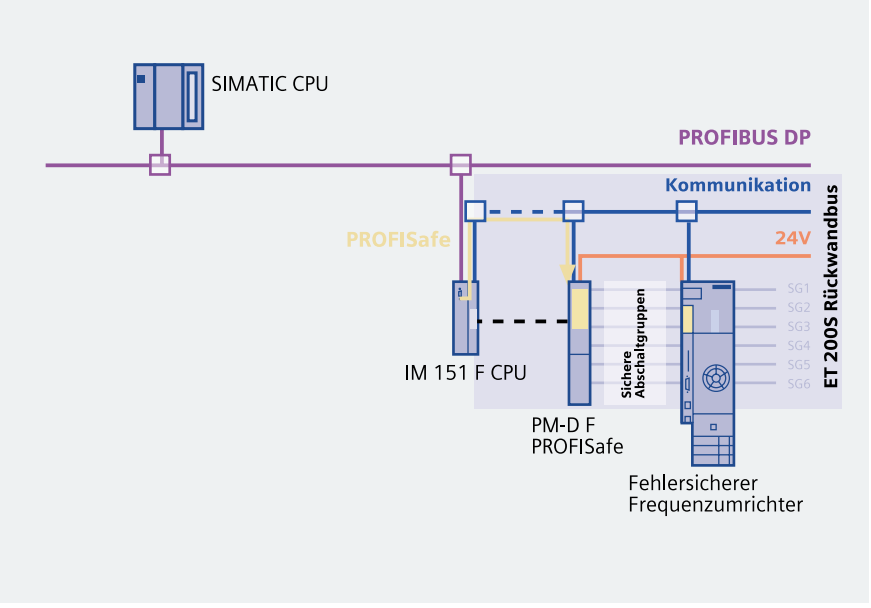
- **Ansteuerung der Sicherheitsfunktionen über PROFIsafe**



Auswertung sicherheitsgerichteter Signale durch eine zentrale fehlersichere CPU und Ansteuerung der fehlersicheren Funktionen des Frequenzumrichters ET 200S FC über das Powermodul PM-D F PROFIsafe.

Zur Weiterleitung der PROFIsafe-Kommunikation an den Rückwandbus der ET 200S wird das Interface Modul IM 151 High feature eingesetzt.

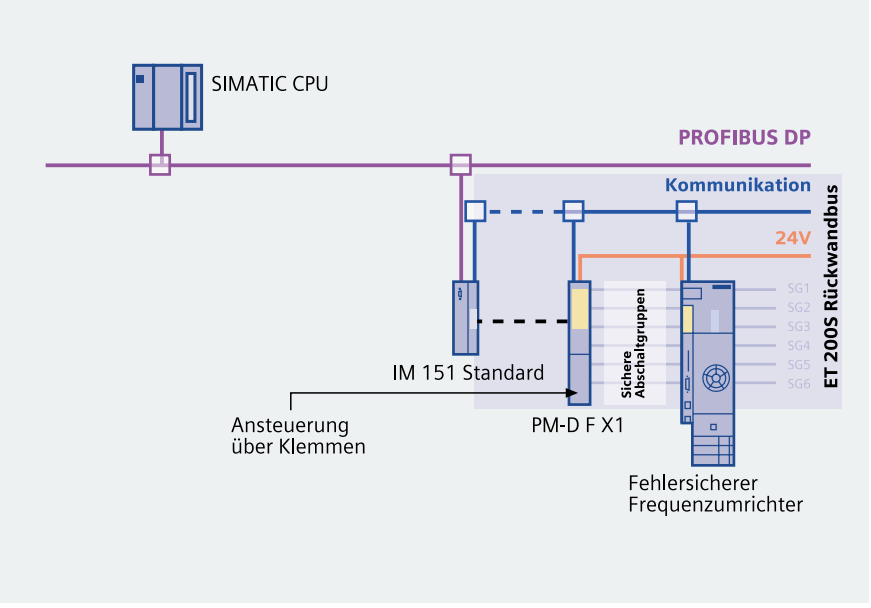
- **Ansteuerung der Sicherheitsfunktionen mit einer fehlersicheren IM 151-7 F-CPU**



Ein Interface Modul mit integrierter fehlersicherer CPU (IM 151-7 F-CPU) erlaubt die Auswertung fehlersicherer Eingangsmodule und die Ansteuerung des Frequenzumrichters innerhalb der ET 200S-Station, wodurch schnellste Reaktionszeiten gewährleistet sind.

In dieser Konfiguration ist keine fehlersichere zentrale CPU erforderlich.

- **Direkte, konventionelle Ansteuerung der Sicherheitsfunktionen**



Eine konventionelle lokale Lösung zur Ansteuerung der Sicherheitsfunktionen ist mit einem Powermodul PM-D F X1 möglich.

Die Abschaltgruppen werden direkt über die Klemmen des Powermoduls PM-D F X1 gespeist, beispielsweise von einem externen 3TK28-Gerät.

Bei dieser Lösung kann jedes beliebige Interface Modul IM 151 eingesetzt werden. Eine fehlersichere CPU ist weder innerhalb der ET 200S noch zentral erforderlich.

Technische Daten

Fehlersicherer Frequenzumrichter SIMATIC ET 200S FC	
Erreichbare Sicherheitsklassen	• Bis Kategorie 3 nach EN 954-1 • Bis SIL 2 nach IEC 61508
Sicherheitsfunktionen	• Sicherer Halt • Sichere Bremsrampe • Sicher reduzierte Geschwindigkeit
Schutzart	IP20
Weitere Features	• Sicherheitsfunktionen an geberlosen Normasynchronmotoren • Modularer Aufbau in dezentraler Peripherie ET 200S • Standard- und fehlersichere Frequenzumrichter in einer Station betreibbar • Fehlersichere und Standard-Eingänge über ET 200S Station • Generatorischer Betrieb mit Netzrückspeisung ohne Chopper oder Bremswiderstand • U/f Steuerung • Vektorregelung mit und ohne Geber • Momentenregelung

10.1 Fehlersichere SIMATIC Controller im Rohbau von Opel Belgien
10.2 Sicherheitstechnik bei Toyota Kanada
10.3 Karosseriebau mit dezentraler Sicherheit bei Ford Australien
10.4 SPS-basiertes Sicherheitskonzept in der LKW-Räderfertigung bei Michelin Deutschland
10.5 Wilde Fahrt bei Madame Tussauds
10.6 Saatgutaufbereitung – Steuerung einer Pumpanlage für Chemikalien mit ASIsafe

10 Referenzen

10.7 AS-Interface vereinfacht Arbeitsschutz bei UPS
10.8 CROWN Vourles – Verpackungsindustrie sicher mit Safety Motorstarter Solution PROFIsafe
10.9 Mehr Sicherheit in der Automobilindustrie
10.10 Neuer Standard für Werkzeugmaschinen
10.11 Sicherheit bei der Produktprüfung von Arbeitsschutztechnik
10.12 Sicherheit und Taktgefühl
10.13 Sicherer Halt in der Druckindustrie

10 Referenzen

10.1 Fehlersichere SIMATIC Controller im Rohbau von Opel Belgien

Bei Opel Antwerpen/Belgien wurde kürzlich ein erstes Automatisierungs- und Sicherheitsprojekt auf Basis von Saftey Integrated mit fehlersicheren Simatic Controllern realisiert. Ausschlaggebend für den Erfolg des Projektes war neben der einmaligen Safety Integrated-Technologie von Siemens auch die sehr enge Zusammenarbeit zwischen dem Engineeringteam von Opel in Antwerpen, dem Systemintgrator Imtech und Siemens Automation and Drives.

Opel Belgium n.v., ein wichtiger Opel-Standort im Hafengebiet von Antwerpen und einer der Kronjuwelen der belgischen Automobilmontage, baut zurzeit verschiedene Varianten des Opel Astra für mehr als 100 internationale Bestimmungsorte.

Vom Sicherheitsrelais zur fehlersicheren Steuerung

Für Francis Luyckx, verantwortlich für das Engineering für den Rohbau bei Opel Belgien, stellt sich die Situation vor der Erneuerung so dar: „Im Body Shop werden alle Maschinen- und Transportbewegungen (von Robotern oder conveoyers), die Gefahren bringen könnten, durch Sicherheitszellen, Lichtvorhänge, sichere Zugangsschalter und Notstopps gesichert. All dies jedoch nach wie vor gesteuert mit Relaisschaltungen.

„Das wollten wir ändern", fährt Francis Luyckx fort. „Und dabei ging es eigentlich um zwei Projekte, oder besser gesagt um ein Doppelprojekt: Zum einen mussten die Roboter, die neu installiert wurden, mit einer Steuerung und einem Sicherheitssystem ausgestattet werden, während zum anderen das bestehende Steuerungs- und Sicherheitssystem ersetzt werden musste. Denn die alte, auf Sicherheitsrelais basierende Installation war nicht nur schon häufig auf veränderte Randbedingungen angepasst worden. Inzwischen war es auch nicht mehr möglich, mit diesem System den neuesten Sicherheitsnormen zu entsprechen und die gewünschten dazukommenden Sicherheitsfunktionen zu erreichen."

Die Kombination von neuen Sicherheitsnormen und neuer Funktionalität, besonders bezüglich einer sehr detaillierten und zuverlässigen Fehlermeldung, sollte auch möglichst leicht erweitert werden können und günstige Life Cycle-Kosten mitbringen. Francis Luyckx dazu: „Die Entscheidung zwischen einem System mit getrennter SPS für die Steuerung und Sicherheitsrelais für die Sicherheit einerseits und einer echten fehlersicheren Steuerung andererseits war schnell getroffen: Letzteres ist nicht nur flexibler, es liefert auch Fehlermeldungen bis hinunter zum fehlerhaften Draht. Und schließlich fällt das Ganze auch noch preiswerter aus."

Eine fast selbstverständliche Wahl ...

„Speziell haben wir uns für die Lösung von Siemens entschieden. Die Gründe waren sehr überzeugend: Zunächst sind wir hier bei Opel schon sehr stark auf den Profibus fokussiert. Neben den positiven Erfahrungen mit diesem Feldbus haben wir inzwischen intern auch ein ansehnliches Paket an Erfahrung rund um den Profibus aufgebaut. Da uns jetzt via Siemens die neue Safety Integrated-Technologie zur Verfügung steht, ist die Entscheidung für eine fehlersichere SPS mit vollkommen integrierten Sicherheitsfunktionen evident. Und gratis dazu bekommen wir die eingebaute Offenheit für zukünftige Weiterentwicklungen in der Automatisierungstechnik."

Opel Belgien sieht den Vorteil von Totally Integrated Automation nicht zuletzt aufgrund der spezifischen Merkmale der riesigen Automobilfabrik. Die zahllosen Vorbearbeitungszellen und typischen Zuführsysteme zum Montageband des Opel Astras fordern mehr und mehr kleinere dezentrale Automatisierungseinheiten. Die praktischen Vorteile liegen auf der Hand: Flexibilität, kurze Verdrahtung, großzügige Netzwerkmöglichkeiten und die Integration auf den Profibus. Und – sehr wichtig – man erhält auch die notwendige Zeit, um zu testen. „All das, was offline und dadurch vorneweg passieren kann, ist für uns ein Vorteil," schließt Francis Luyckx ab.

Weitere Verfeinerung

Nun stand die weitergehende Integration der Sicherheitsfunktionen im Pflichtenheft. Dabei ging es zunächst um die Fehlermeldungen. Diese sollten mittels Parametrieren mit der Standard-Software von Siemens auf den Bedienoberflächen der HMI Panels erzeugt werden. Natürlich lassen sich so auch weitere Formen von Sicherheitsintelligenz implementieren, zum Beispiel „muting"-Funktionen (programmierte und sichere Unterdrückung von Sicherheitsfunktionen, was für den normalen Verlauf der Produktionsbewegungen verlangt werden kann) beim Einsatz von Sicherheits-Lichtvorhängen.

Für Eric Moons spielt die E-Mail-Karte ein sehr zentrale Rolle, die in der fehlersicheren SPS sitzt. „Die zentralen Sicherheitsdienste von Opel Antwerpen haben dadurch, wie gefordert, eine neue Bewachungsmöglichkeit der Sicherheitssoftware. Sobald nämlich die Sicherheitssoftware geändert wird, wird automatisch eine E-Mail an den Sicherheitsdienst gesendet."

Die Spezialisten von Siemens Automation & Drives übernahmen zusammen mit dem Maschinenbauer Comau die Inbetriebnahme und Programmierung der ersten fehlersicheren SIMATIC S7-315F. Der Systemintegrator Imtech übernahm – selbständig und problemlos – die zweite fehlersichere Steuerung vom Typ S7-416F. Wim Van Goethem, Projektingenieur bei Imtech, schildert seine Erfahrungen so: „Mit Hilfe eines Trainings von Siemens konnten wir die Basis schaffen, um die vollständige Programmierung und Implementierung sehr schnell über die Bühne zu bringen."

Die positiven Erfahrungen des Opel-Teams nach zwei Monaten, in denen das System im Einsatz ist, sprechen für sich: „Das System ist eingesetzt und gestartet worden und ... wir haben es sprichwörtlich prompt vergessen" beschreibt Francis Luycks, die Situation. „Es arbeitet völlig reibungslos – ohne dass ein einziges Problem aufgetaucht wäre. Wir wollen und müssen uns jetzt nur noch richtig daran gewöhnen, dass wir ein System haben, in dem die Sicherheit echt und vollständig integriert ist. Früher mussten die Sicherheitsfunktionen separat programmiert werden und waren dadurch eher explizit zu sehen. Jetzt sitzt alles im System. Das wissen wir sehr wohl, aber ab und zu überkommt einen doch noch der Reflex, sich alles nochmals separat anzuschauen – quasi als ob man sehen will, dass die Norm 61204 erfüllt ist."

Beim Einsatz in der Fertigungshalle

Beide fehlersicheren SIMATIC Controller werden im Bereich Rohbau (metal finish) eingesetzt. Hier wird die Rohkarosserie des Autos hergestellt. Der eine fehlersichere Controller bedient die Funktionen des Punktschweißens (stud welding) sowie das Transportsystem, mit dem die Karosse dorthin transportiert wird, wo Kofferraumdeckel oder Rücktür montiert werden.

Die zweite fehlersichere Steuerung ist dort im Einsatz, wo nachgearbeitet wird, wie beispielsweise Polieren, die visuelle Kontrolle der Oberflächenqualität oder das so genannte „fitting". Dies umfasst das Einpassen und Öffnen der Türen sowie das Öffnen des Kofferraumdeckels, bevor die Karosserie in die Lackierstraße befördert wird. Beide Systeme fordern raumgreifende und komplexe Transportbewegungen. Hinzu kommt auch noch die hochspezialisierte Handarbeit der Facharbeiter, so dass die zahlreichen gefahrbringenden Bewegungen zuverlässig abgesichert werden müssen.

„Die physikalischen Absicherungen bestehen aus Reißleinen, normalen Notstopp-Schaltern, Lichtvorhängen mit und ohne „muting"-Funktionen und klassischen Sicherheitszellen mit Sicherheitsschlössern", erläutert Francis Luyckx. „Ein sehr komplexer Zustand, mit dem die fehlersichere SIMATIC bestens zurechtkommt. Denn sie kontrolliert das alles und kommuniziert über einen Profibus DP/DP-Koppler mit den normalen Steuerungen. Im Laufe des Jahres möchten wir mit einem nächsten Schritt dieses allerdings quasi überflüssig machen. Denn dann soll ein und dieselbe fehlersichere SIMATIC-Steuerung sowohl die Sicherheitssteuerung als auch die normale Steuerung des Fertigungsprozesses übernehmen."

(aus move-up 1-2/2003)

10.2 Sicherheitstechnik bei Toyota Kanada

Für das neue Lexus-Werk und eine Anlagennachrüstung entschied sich Toyota Kanada für eine Sicherheitslösung mit Siemens AS-Interface at Work und SIMATIC S7-300F. Neben erhöhter Sicherheit profitiert der Autobauer von höherer Verfügbarkeit und steigert damit seine Produktivität.

Toyota Motor Manufacturing Cambridge (TMMC) im Süden der kanadischen Provinz Ontario ist ein echtes automobiles Aushängeschild. Es ist ständig unter den Top 10 der JD Power and Associates zu finden und wurde jüngst mit einer ganz besonderen Auszeichnung der Muttergesellschaft bedacht: Es ist das erste Werk außerhalb Japans, in dem ein Modell aus der Lexus-Reihe, der brandneue Luxus-Offroader RX 330, gebaut werden soll.

Für das neue Lexus-Werk sowie das bestehende Corolla-Werk kommen jetzt Sicherheitssysteme zum Einsatz, die neben maximaler Sicherheit auch verbesserte Diagnosemöglichkeiten bieten und so eine Produktionssteigerung ermöglichen. Zusammen mit Siemens Kanada und dem Ingenieurbüro Stantec entwickelte TMMC eine richtungsweisende Lösung mit AS-Interface Safety at Work und fehlersicheren SPS SIMATIC S7-300F. Diese wird kostengünstig sowohl für das neue Lexus-Werk als auch für die Nachrüstung des Corolla-Werks eingesetzt.

Ondrej Benjik, bei Siemens für das Safety-Projekt verantwortlich, hat zusammen mit dem TMMC-Projektmanager Scott Bartlett die Retrofit-Strategie festgelegt. Er erinnert sich: „Wichtig bei der Nachrüstung war, dass die neue Sicherheitslösung in die vorhandene Steuerungsplattform integriert werden konnte. Vorhandene Feldgeräte und Verkabelungen sollten ersetzt werden. Die Umrüstung sollte ohne oder nur mit einer stark begrenzten und planbaren Produktionsunterbrechung umzusetzen sein. Außerdem legte Toyota Wert auf Effizienz im Einsatz, zum

Beispiel durch schnelle Behebung von Betriebsstörungen.

Alle Sicherheitsbestimmungen erfüllt

Die Siemens Aktor-Sensor Interface-Produkte haben sich als besonders gut geeignet für diese Aufgabe erwiesen. Die Anforderungen der kanadischen Arbeitsschutzverordnung, die für alle sicherheitsrelevanten Einrichtungen Sicherheitstests vor Anlauf der Produktion vorschreibt, wurden vollständig erfüllt.

„Die Umstellung ging reibungslos vonstatten", erinnert sich Bartlett, „Die Toyota-Mitarbeiter nahmen das Konzept bereitwillig auf und verstanden sofort die Bedeutung der Anlage." Die Nachrüstung der Roboterzellen in der Corolla-Lackierstraße fand an Wochenenden und während der Werksferien statt, so dass Produktionsstillstände vermieden werden konnten.

Die „Anti-Chip"-Kabine, in der die Schutzlackierung für die Schweller aufgetragen wird, und die „Blackout"-Kabine, in der der Unterbodenschutz aufgebracht wird, wurden mit minimalen Änderungen an der vorhandenen SPS-Steuerung auf die neuen Sicherheitssysteme aufgerüstet. Das AS-Interface-Sicherheitsnetz von Siemens basiert auf einem nicht-proprietären Standard und lässt sich somit problemlos in nahezu jede SPS integrieren. Über AS-Interface können Lichtvorhänge, Laserscanner, Sicherheitsverriegelungen und Notausschalter direkt über einen Bus verbunden werden, wobei die Sicherheitsanforderungen der Kategorie 4 erfüllt werden. Gleichzeitig entfällt durch die einzigartige Direktanschlusstechnologie des AS-Interface-Systems für Sicherheitskomponenten und/oder Sicherheitseingangsmodule auch die Notwendigkeit verteilter I/O-Stationen. Damit reduziert sich der Aufwand für feste Verdrahtung fast auf Null. Durch die einfache Installation verringern sich die Inbetriebnahmekosten und die Nachrüstzeit deutlich. Außerdem werden schon vor der Inbetriebnahme vollständige Funktionstests möglich.

SIMATIC S7-300F für den Lexus

Das neue Lexus RX 330-Werk arbeitet mit Siemens-Sicherheitslösungen, die den EN 954-1- und IEC 61508-Standard erfüllen. Das AS-Interface wird im neuen Paint Shop eingesetzt. Im Karosserierohbau findet die fehlersichere SPS-Steuerung SIMATIC S7-300F auf Profibus Verwendung.

„Die Installation bei Toyota hat bewiesen, dass die besten Sicherheitslösungen nicht nur für eine bessere Arbeitssicherheit sorgen", fasst Benjik von Siemens zusammen, „sondern dass damit auch wirtschaftliche Ziele wie hohe Verfügbarkeit und eine schnelle Fehlerbehebung unterstützt werden."

Toyota Motor Corporation

Die Toyota Motor Corporation ist der drittgrößte Automobilhersteller der Welt und bietet eine komplette Modellpalette von Kleinwagen bis zu großen Lkws an. Insgesamt wurden im Jahr 2001 unter den Markennamen Toyota und Lexus sowie Daihatsu und Hino weltweit 5,94 Millionen Fahrzeuge verkauft. Neben den 12 eigenen Werken in Japan betrieb Toyota im März 2002 weitere 54 Produktionsunternehmen in 27 Ländern und Standorten, in denen Fahrzeuge und Komponenten der Marken Lexus und Toyota von weltweit 246.700 Beschäftigen hergestellt werden (konsolidierte Zahlen) und vertreibt Fahrzeuge in mehr als 160 Ländern und Regionen. Der Automobilsektor und die Verkaufsfinanzierung haben einen Anteil von mehr als 90 Prozent am Gesamtumsatz des Unternehmens. Zu den weiteren Tätigkeitsbereichen zählen Telekommunikation, Fertighäuser und Freizeitboote.

Toyota Mini-Van-Fertigung failsafe

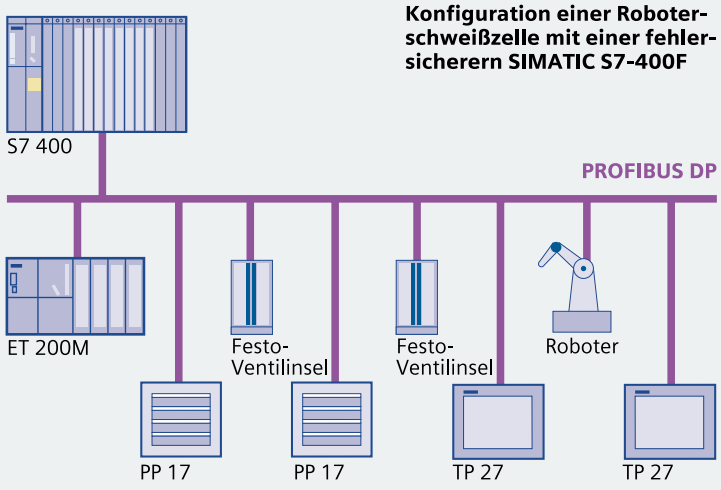
Nach einer langen und intensiven Erprobungsphase entschied sich Toyota beim Karosserierohbau des neuen Mini-Van „Sienna" für den Einsatz einer neuen Failsafe-Technologie auf Basis von fehlersicheren SIMATIC S7-SPS-Steuerungen und PROFIsafe. Da eine Produktionslinie aufgrund von Modellwechseln ständig modifiziert wird, ermöglicht die Lösung mit verteilten Sicherheits-SPS-Steuerungen eine schnelle, einfache und kostengünstige Produktionsumstellung. Die Auswertung von Toyota ergab darüber hinaus, dass die SIMATIC Failsafe-Steuerung hinsichtlich Funktionalität und Zuverlässigkeit in automatisierten Linien im Vergleich zu den Sicherheits-SPS-Steuerungen vieler anderer Hersteller die effizienteste Lösung darstellt. Derzeit laufen Projekte in drei Toyota-Werken weltweit: Tahara (Japan), Indiana (USA) und Cambridge (Kanada). Insgesamt kommen in allen drei Werken zusammen 170 SPS-Steuerungen mit etwa 2000 Sicherheits-I/O-Modulen zum Einsatz.

(aus move-up 3/2003)

10.3 Karosseriebau mit dezentraler Sicherheit bei Ford Australien

Das Sicherheitssystem für die neuen Schweißzellen für Karosserie-Rohbauteile im Ford-Werk Geelong, Australien, ist mit fehlersicherer SPS-Technologie von SIMATIC und PROFIsafe ausgestattet. Die effektive Anwendung der dezentralen Peripherie über Profibus führte zu Zellen mit einem Minimum an verdrahteten Komponenten und Feldverkabelung sowie zu ausgezeichneten Diagnosemöglichkeiten.

Das Aushängeschild von Ford Australien ist der BA „Falcon“. Die Limousine mit Sechszylinder-Motor wurde vollständig in Australien konstruiert und läuft seit Oktober 2002 im Werk Victoria vom Band. Karosserieteile für den „Falcon“ werden im Ford-Werk Geelong im Südwesten Melbournes gefertigt. Das Geelong-Werk war in der Vergangenheit mit SPSen verschiedener Hersteller ausgerüstet. Zu Beginn der Planung der Fertigungsausrüstung für das neue Modell wurden zahlreiche Automatisierungstechnologien untersucht, um eine zukunftsfähige Automatisierungsplattform zu finden. Ford suchte eine flexible Plattform, die für die Instandhalter einfach zu programmieren und zu diagnostizieren ist. Das neue System sollte problemlos die bereits vorhandenen Komponenten von Drittanbietern, wie Roboter und Ventilinseln, integrieren.



Konfiguration einer Roboterschweißzelle mit einer fehlersicherern SIMATIC S7-400F

SIMATIC gewählt

Detaillierte Untersuchungen und Tests führten schließlich zur Entscheidung für das Produktspektrum der SIMATIC-Reihe. Zunächst ging es an die Auswahl des Sicherheitssystems. Wurde früher für die Sicherheit der Zelle eine Kombination aus konventionell verdrahteten Sicherheitsrelais verwendet, prüfte Ford jetzt Konzepte für den Einsatz der neuen fehlersicheren SPS SIMATIC S7-400F als Alternative. Hier lieferte der örtliche Siemens Solution Provider Industrial Control Technology pty Ltd (ICT) Unterstützung. Dabei arbeitete ICT eng mit Siemens Australien und einem Spezialisten des Competence Center Automotive (CCA) von Siemens A&D in Nürnberg zusammen.

Das Ergebnis war ein elegantes Designkonzept, das einheitlich auf alle sechs neuen Zellen angewendet werden konnte und einen großen Prozentsatz von Relais und aufwändigen Zwischenverkablungen einsparte. Sicherheitsfunktionen konnten auch für die bestehenden Zellen angewendet werden. Außerdem wurden weitere Sicherheitseinrichtungen und automatische Prüfungen hinzugefügt, die besonders die Wartung und Inbetriebnahme erleichtern, beispielsweise die ausführliche Diagnostik auf den Touch Panels, die die Fehlersuche erheblich vereinfacht.

Die Zellen sind hauptsächlich für das Roboterschweißen vorgesehen. Gepresste Karosserieteile werden den Bearbeitungsstationen zugeführt und dort punktgeschweißt. In einigen Fällen werden die Werkstücke mit Hilfe von Robotern für weitere Bearbeitungen zu anderen Aufspannungen befördert. Die Ford-Ingenieure haben die SIMATIC-Bedien- und Beobachtungssysteme und dezentrale Peripherie mit Profibus bestmöglich für das Design der Zellen genutzt. Die Roboter werden direkt über Profibus angesteuert und erlauben so einen schnellen und reibungslosen Datenverkehr. Pneumatische Komponenten an den Aufspannungen sind über Festo-Ventilinseln an den Profibus angeschlossen.

Für die Werkerbedienung und Visualisierung sind die Bedienstationen mit Operator Panels PP17 ausgestattet. Darüber hinaus erlauben die eingesetzten Touch Panel TP 27 den Zugang zu Produktionsdaten und Diagnoseinformationen. Auf den größeren Zellen liefert ein Touch Panel MP 370 diese Daten und Informationen zusätzlich an einer zentralen Stelle.

Die hoch auflösende Grafik dieser Panels ermöglichen die Darstellung von realen Fotos der Aufspannungen mit darüber angezeigtem dynamischem Status der einzelnen Spanner und Näherungsschalter – eine vorteilhafte Methode, dem Werker Diagnoseinformationen zu liefern.

Sicherheitssysteme zentral mit SIMATIC S7-400F

Die Automatisierungsfunktionen der Zellen werden vom Standard-, also nicht fehlersicheren Kontaktplan-(KOP)-Code in der SIMATIC SPS S7-400F übernommen, die eng mit den Roboterprogrammmen verknüpft ist. Ford-Mitarbeiter programmieren die Roboter nach den Prozesserfordernissen und um mit der überwachenden SPS zu interagieren. Die Entwicklung von Standard-Codes für die SPS ist in den meisten Fällen von ICT in enger Zusammenarbeit mit Ford durchgeführt worden. Spätere Zellen haben Ford-Mitarbeiter dann selbst inhouse projektiert. Natürlich sind die Sicherheitssysteme ein kritischer Bestandteil dieser Zellen. Üblich sind Lichtgitter für jede Zelle. Lichtschranken schützen die Arbeitsplätze, an denen Teile von Hand aufgelegt werden. Mit der Zweihandsteuerung kann ein Teil eingespannt werden, während der Werker innerhalb des mit Lichtschranken gesicherten Bereichs bleibt. Positionsschalter am Robotersockel überwachen die Ausrichtung und erlauben so den manuellen Zugriff zu einer Aufspannung, während der Roboter gerade an einer anderen arbeitet. Lichtschranken schützen auch die Zugangspunkte für Gabelstapler, wenn diese fertige Teile auf Paletten abholen.

Sicherheitsverriegelungen in den Robotern, den Sensoren in den Aufspannungen, den Antrieben für die Servo-Drehtische und in einem übergeordneten Schnellentlüftungsventil reagieren auf die Signale von Lichtschranken, Zugangstoren und Not-Aus. All diese Sicherheitsfunktionen sind über eine fehlersichere SPS SIMATIC S7-400F implementiert. Auch die elektrische Verriegelung am Zugangstor wird von einer Sicherheits-SPS gesteuert. Die Implementierung dieser Funktionen über Software hat zu einer drastischen Verringerung der Schaltschrankverkabelung geführt und ist eine praxisgerechte Umsetzung der benötigten Sicherheitslogik.

Neue Wartungsfunktionen konnten hinzugefügt werden, die mit dem vorherigen konventionell verdrahteten System unmöglich gewesen wären. Diagnosefunktionen auf den SIMATIC Touch Panels TP 27 liefern detaillierte Informationen über den Status des Sicherheitssystems und die Fehlerdiagnose. Eine Hauptanforderung von Ford war, den Zugriff auf die programmierten Sicherheitsfunktionen zu sperren, gleichzeitig jedoch freien Zugang zum Standard-Code zu behalten. Dies ist wichtig, da von Zeit zu Zeit Modifikationen benötigt und zusätzliche Systeme an den Linien installiert werden, während die Sicherheitsfunktionen typischerweise konstant bleiben. Dies wurde problemlos mit der SIMATIC S7-400F erreicht. Jetzt ist es möglich, den Standard-Code zu ändern, ohne den Failsafe-Code zu beeinflussen.

Dezentrale Sicherheit in KOP

Die neueste Installation der dezentralen Sicherheitstechnik ist in KOP programmiert und basiert auf „Distributed Safety". Sie wird von den Ford-Mitarbeitern gut angenommen. Die Programmierung der fehlersicheren Logik in KOP wird als einfachere Alternative zu CFC gesehen, die in früheren S7-400F-Systemen eingesetzt wurde. Für alle zukünftigen Systeme will Ford KOP verwenden.

Ford hat bereits angekündigt, dass man die SIMATIC S7-315F auch bei Sicherheitsperipherie für kleinere Maschinen einsetzen will, die eigentlich nur ein oder zwei Sicherheitsrelais benötigen. Diese SPS ist extrem kosteneffizient und leistungsfähig. Jüngst wurde mit der Projektierung von fünf neuen Zellen begonnen. Auch für diese Zellen wird die dezentrale Sicherheits-SPS S7-315 für alle Automatisierungs- und Sicherheitsfunktionen zum Einsatz kommen.

(aus move up 1-2/2003)

10.4 SPS-basiertes Sicherheitskonzept in der LKW-Räderfertigung bei Michelin Deutschland

Europas führender Hersteller von LKW-Stahlrädern sah sich mit der Aufgabe konfrontiert, seine bewährte Felgenprofilierlinie nachträglich auf den Standard der höchsten Sicherheitskategorie 4 nach DIN EN 954-1 nachzurüsten. Diese Aufgabe schien angesichts der Komplexität der Anlage mit herkömmlicher Sicherheitstechnik nahezu unlösbar, ließ sich aber mit fehlersicherer SPS- und Feldbustechnik schnell und hoch flexibel bewältigen.

Aus der Stahlstadt Solingen kommen nicht nur messerscharfe Klingen, von dort aus gehen auch Millionen von Rädern für Pkws und Lkws in alle Welt. Als Rad bezeichnen die Hersteller, was dem Autofahrer eher als Felge geläufig ist: Eine Verbindung aus der so genannten Schüssel, die an der Nabe befestigt wird, und der den Reifen tragenden Felge. Beide Teile werden separat vom Blech-Coil gefertigt, dabei in mehreren Stufen geformt, gestanzt, gefügt, miteinander verschweißt, geprüft und lackiert. Branchenprimus bei Lkw-Stahlrädern in Europa ist Michelin bei einem Marktanteil von ca. 50 Prozent. Die Geschäftseinheit "Räder" des Pneu-Erfinders fertigt diese für die Sicherheit aller Verkehrsteilnehmer sehr wichtigen Teile in Stückzahlen von jährlich weit über zwei Millionen. Produziert wird an den Standorten Troyes (Frankreich), Aranda de Duero (Spanien) und seit 1997 auch in Solingen. In der Stahlstadt fertigt die Michelin Kronprinz Werke GmbH auf derzeit drei Schüsselstraßen und einer Felgenlinie jährlich rund 600.000 Lkw-Stahlräder. Diese Ausbringung soll sich in den nächsten drei Jahren verdoppeln, wenn Solingen zum Entwicklungszentrum avancieren und schrittweise die Kapazitäten der spanischen Tochter übernehmen wird.

Sicherheitstechnik neu aufgebaut

Bei aller Produktivität stellt die Konzernmutter höchste Ansprüche an die Arbeitssicherheit. Das erklärte Ziel: weniger als fünf Arbeitsunfälle je Werk und Jahr. Um diesen Wert langfristig zu erreichen, wurde auch die schon seit mehreren Jahren produzierende Felgenprofilierlinie bei Kronprinz einer detaillierten Risikoanalyse unterzogen. Ergebnis: Auf die Linie aus drei Umformanlagen ist die Sicherheitskategorie 4 nach DIN EN 954-1 anzuwenden und sie muss sicherheitstechnisch „runderneuert" werden.

Drei Schutzbereiche waren zu realisieren, und insgesamt mussten 24 Schutztüren, zwölf Pressensicherheitsmodule sowie 30 Motoren in ein durchgängiges Sicherheitskonzept integriert werden. Mit der Durchführung wurde die Ingenieurgemeinschaft Europlan Systemtechnik aus Kempen bei Krefeld betraut, die ähnliche Aufgaben schon mehrmals gelöst hat. Bislang allerdings immer auf konventionelle Weise, also mit fester Verdrahtung, Sicherheitssteuerung und eigenem Sicherheitsbus – was bei fast 60 Sicherheitsrelais keine leichte Aufgabe zu werden versprach.

In die Phase der Vorplanung fiel eine Präsentation der neuen fehlersicheren SPS-Steuerungen von Siemens. „Auf Anhieb überzeugend waren für mich vor allem die umfassenden Möglichkeiten zur Fehlerdiagnose und die Flexibilität", so Dipl.-Ing. Siegfried Schädlich, Leiter der Elektroplanung der Geschäftseinheit Räder „weshalb wir das kalkulierbare Risiko eingegangen sind und unsere erste SPS- und feldbusbasierte Sicherheitslösung realisiert haben."

Verteiltes System für ganzheitliche Sicherheit

Herzstück des neuen, aus Zeit- und Kostengründen parallel zur vorhandenen Liniensteuerung aufgebauten Safety-Konzepts ist eine fehlersichere SIMATIC S7-300F. Grundsätzlich können auf einer SIMATIC F-CPU „normale" und sicherheitsgerichtete Aufgaben nebeneinander realisiert werden, bei Kronprinz verarbeitet die F-CPU (S7-315F) aber ausschließlich sicherheitsrelevante Feldsignale. Sie schaltet die Anlage bzw. den Anlagenabschnitt bei Fehlern sofort in einen sicheren Zustand. Statt über eine Vielzahl von Einzeladern werden die Sicherheitseinrichtungen über eine sichere Profibus-Verbindung an die CPU gekoppelt. In der Nähe der Schutzeinrichtungen (Schutztüren, Pressensicherheitsmodule) gibt es kleine Vor-Ort-Schaltkästen mit fehlersicheren Signalmodulen SIMATIC ET 200S Profisafe, die die lokalen Signale über herkömmliche Profibus-Kabel an die Zentrale im Schaltraum übermitteln. Die fehlersichere Kommunikation gewährleistet das von der PNO entwickelte Protokollprofil „Profisafe", das mit SIL 3 (IEC 61508) und der Kategorie 4 der EN 954-1 höchste Sicherheitsanforderungen erfüllt.

Mechanische Verriegelungen an den Schutztüren und zusätzliche Abfragen im Steuerungsprogramm verhindern, dass die Produktion unbeabsichtigt unterbrochen werden kann. Die für diese Abstimmung der Sicherheitseinrichtungen mit dem Produktionsprozess notwendige Brücke zur (SIMATIC-) Liniensteuerung hat Europlan per Buskopplung geschlagen.

„Einer der grundlegenden Vorteile SPS-basierter Lösungen ist natürlich die Flexibilität", so Siegfried Schädlich „denn wie die Praxis zeigt, lässt sich nur selten alles exakt im Voraus planen, und oft kommen erst bei der Inbetriebnahme zusätzliche Wünsche und Aufgaben auf den Entwickler zu. Diese nachträglich geäußerten Wünsche können wir mit SIMATIC F-Controllern künftig auch in der Sicherheitstechnik schnell und flexibel erfüllen." Mit fest verdrahteten Sicherheitsrelais sind vermeintlich geringfügige Änderungen immer mit höherem Zeitaufwand verbunden, zusätzliche Forderungen sogar oft nur mit überproportionalem Aufwand zu realisieren, während allein schon die Anbindung der Schutzeinrichtungen per Profibus große Flexibilität für Erweiterungen schafft. „Eine Zeit sparende Rolle spielt dabei auch die schon während der Inbetriebnahme mögliche Visualisierung aller Zustände und Komponenten auf einem HMI-Gerät", so Programmierer Mario Stärz von Europlan. Beim konventionellen Ansatz sind viele Informationen in diesem frühen Projektstadium nur durch zeitraubendes Messen von Einzelsignalen zu erhalten.

Seit Anfang 2003 liefert ein SIMATIC Touch Panel TP270 im Schaltschrank vor Ort laufend detaillierte Informationen über den aktuellen Status der Anlagensicherheit. In die Bedienoberfläche integriert ist auch das standardisierte Profibus-Diagnosemodul von Siemens, um Störungen schnell lokalisieren und beheben zu können. Das macht die Diagnose sehr einfach, hält die Stillstandszeiten kurz und damit die Verfügbarkeit hoch.

Engineering wie gewohnt

Als Einsteiger in die SPS-basierte Sicherheitstechnik hat Mario Stärz ausschließlich das Software-Optionspaket „Distributed Safety" für Step7 genutzt. Diese Bibliothek enthält TÜV-zertifizierte Baustein- und Applikationsvorlagen für sicherheitsgerichtete Aufgaben. Sie ist eingebettet in die Step-7-Umgebung, so dass sich in den Standardsprachen F-KOP (Kontaktplan) und F-FUP (Funktionsplan) auch anspruchsvolle Sicherheitsaufgaben schnell und sicher lösen lassen. „Damit waren unterschiedliche Funktionalitäten für die Betriebsarten Einrichten und Automatik ebenso einfach zu realisieren wie das flexible Gruppieren bestimmter Anlagenteile für einen gefahrlosen Werkzeugwechsel oder das Nachbearbeiten (Schmirgeln) von Werkzeugen in der Linie", so der Programmierer. Wem der mitgelieferte Funktionsumfang nicht ausreicht, der kann die Möglichkeiten des offenen Systems voll nutzen und Bausteine modifizieren oder aus dem Befehlsvorrat des Optionspakets eigene Bausteine generieren.

Die Maschinenführer wissen die hohe Transparenz und die einfache, komfortable Bedienung der neuen Sicherheitstechnik per Touch Panel zu schätzen. Die Diagnosefähigkeiten konnten bislang noch nicht in der Praxis unter Beweis gestellt werden, da es noch keinen einzigen Fehler, wie Drahtbruch, Kurz- oder Querschluss, in den sicherheitsgerichteten Anlagenteilen gegeben hat.

Die für technisch und wirtschaftlich effiziente Umsetzung der Sicherheitsanforderungen Verantwortlichen bei Michelin Kronprinz sehen den SPS-basierten Ansatz mit SIMATIC F-Controllern mittlerweile auch bei deutlich kleineren Anlagen eindeutig im Vorteil: „Schon bei zwei Schutzkreisen innerhalb einer Anlage macht der Performancegewinn in der Anwendung die etwas höheren Investitionskosten wett", ist Siegfried Schädlich überzeugt. So stehen er und die Firma Europlan bereits mitten in der Detailplanung für einige weitere Projekte, unter anderem für die SIMATIC-gesteuerte Sicherheitstechnik einer neuen, komplexen Schweißstrecke für Pkw-Räder.

(aus Blech Rohre Profile, Ausgabe 8/03)

10.5 Wilde Fahrt bei Madame Tussauds

In die Betriebsautomatisierung integriertes Sicherheitssystem

Moderne Fahrgeschäfte und Produktionseinrichtungen haben einiges gemeinsam: Hier wie dort sorgen dynamische Antriebe für automatisierte Bewegungen. Und: Stillstand ist absolut unerwünscht, sonst geht die Wirtschaftlichkeit in den Keller. Dennoch soll bei allem Streben nach Umsatz, die Sicherheit der Menschen an oberster Stelle stehen.

Ein Besuch bei Madame Tussauds in London umfasst neben der obligatorischen Wachsfigurenausstellung auch eine so genannte „Spirit of London"-Fahrt. Besucher werden auf eine Zeitreise geschickt, in der sie London von seinen frühen Anfängen bis in die Gegenwart erleben. In einem von 87 Londoner Taxis „fahren" Passagiere durch die Geschichte Londons. Damit ihnen dabei nichts zustößt, hat Siemens Automation and Drives (A&D) die Sicherheit und Kontrolle der Erlebnisfahrt auf den neuesten Stand der Sicherheitstechnik gebracht.

Bei Madame Tussauds sorgt moderne Technik für Sicherheit

Interdisziplinäre Technik

Der Leistungsumfang der Anlage ist sehr vielschichtig und umfasst jede Menge mechanischer und elektrischer Antriebe, synchronisierte Beleuchtung, Klang- und Spezialeffekte sowie eine gezielte mehrsprachige Erläuterung. Um dieses einzigartige Indoor-Fahrgeschäft aufzubauen, wurden die verschiedenen Technologien automatisierter, fahrerloser Systeme, der Industrieautomatisierung und der Theaterwerkstätten kombiniert. Die Sicherheitssysteme sind so konzipiert, dass sie bei jeder Störung Sicherheit gewährleisten können – egal ob diese durch die Anlage selbst, durch die Besucher oder äußere Ereignisse ausgelöst wurde.

Die Betreiber von Madame Tussauds haben das lokale Ingenieurbüro D.B. Brooks, das sich auf Fahrgeschäfte spezialisiert hat, beauftragt, einen detaillierten Entwurf für die erforderliche Sicherheitstechnik zu erstellen. Eine gemeinsame Überprüfung der Alternativen hat schnell gezeigt, dass die Installation von Siemens AS-Interface Safety at Work (im System AS-Interface integrierte Sicherheitstechnik) die Kombination von höchstmöglicher Sicherheit und Zuverlässigkeit bei betrieblicher Flexibilität erlaubt. Möglich ist dies durch die Einführung der neuen internationalen Standards EN 954-1 und IEC, die jetzt erlauben, dass alle Sicherheits- und Betriebsführungssysteme vollständig integriert werden können.

Zertifizierte Sicherheit

Mit AS-Interface Safety at Work werden diese technischen Voraussetzungen erfüllt und in die Praxis umgesetzt. Dabei setzen Sicherheitsfunktionen so weit wie möglich auf Komponenten der seit Jahren bewährten Betriebsautomation auf. Im Fall des AS-Interface werden auf hardwaremäßig unveränderten Kommunikationswegen neben den Signalen der Betriebsautomation nun parallel auch die Signale mit Sicherheitsverantwortung übertragen. Eigens entwickelte und zertifizierte Sicherheitsbauteile zum Senden, Empfangen und Auswerten der sicheren Signale sind mit dem bestehenden Kommunikationskonzept kompatibel. Dies ermöglicht durch Einsparung bei Verdrahtung und einfacherer Diagnose einen entscheidenden Vorsprung bezüglich der Wirtschaftlichkeit. Die Anwendung bei Madame Tussauds ist vor allem deswegen von besonderer Bedeutung, weil es in England die erste Anwendung von AS-Interface Safety at Work im Bereich der „hochentwickelten Technologiefahrgeschäfte" im Markt der Besucher-Attraktionen ist.

Eine Steuerung SIMATIC S7-300, die zentrale Schaltstelle der neuen Installation, hat über AS-Interface Zugriff auf alle Aktoren und Sensoren und ist zudem mit den sechs Bediengeräten verbunden, die jeden Aspekt der Fahrt kontrollieren. Parallel werden die sicherheitgerichteten Signale kontinuierlich über einen unabhängigen Sicherheitsmonitor ausgewertet

An jedem Einsatzort, geben die Bediengeräte OP7 von Siemens Zugang zu allen Kontrollelementen – von normalen Bedienungs- und Wartungsarbeitsschritten über sicherheitstechnische Elementen bis hin zu Feueralarm- und Evakuierungssystemen. Umfangreiche Diagnoseinformationen sind darin inbegriffen.

Lichtvorhänge der Baureihe SIGUARD, ein Safety-Integrated-Produkt für Anwendungen bis zu EN 954-1 Kategorie 4, errichten ein optisches Schutzfeld, das Personen sicher detektiert, falls diese während der Fahrt aussteigen. Für den Fall, dass eine Notfallsituation eintritt, dauert es weniger als zwei Sekunden, bis das Fahrgeschäft gestoppt ist und die Beleuchtung angeht. Parallel wird die Notfallevakuierung gestartet, die Sicherheitsbeleuchtung und Durchsagen beinhaltet.

Integriertes System erhöht die Sicherheit

AS-Interface Safety at work ist ein Teil von Safety Integrated und Safety Integrated ist das Konzept aus dem Hause Siemens, das alle Aspekte der Ablaufsteuerung und des Datenmanagements vereint, um höchstmögliche Sicherheitsstandards für Mensch, Maschine und Umwelt zu bieten. Es ist ein durchgängig in die Betriebsautomatisierung integriertes Sicherheitssystem von Totally Integrated Automation. Durch diesen Ansatz innovativer Sicherheitstechnologie ergeben sich für die Anwender Vorteile in Sachen Wirtschaftlichkeit, Flexibilität und Sicherheit.

10.6 Saatgutaufbereitung – Steuerung einer Pumpenanlage für Chemikalien mit ASIsafe

In einer großen englischen Saatgutaufbereitungsanlage ging vor kurzem eine voll automatisierte, über das gesamte Werksgelände verteilte Pumpensteuerung für die dazu eingesetzten Chemikalien in Betrieb. In Zusammenarbeit mit einem Systemintegrator wurden alle Aspekte einer vollautomatischen, hoch genauen und sicheren Prozesssteuerung mit der geforderten Datenhaltung nach internationalen Standards vereint.

In Zeiten schwindender Agrarflächen kommt dem Flächenertrag und damit der Qualität des eingesetzten Saatgutes immer größere Bedeutung zu. Bayer Cropscience, ein Teil der international tätigen Wynnstay Group, stellt Chemikalien zur Saatgutaufbereitung her und lieferte für die Firma Wynnstay Arable eine sog. „Twin Vanguard"-Saatgutaufbereitungsmaschine.

Wynnstay Arable hat sich auf die Aufbereitung von Saatgut für die landwirtschaftliche Industrie spezialisiert und legt dabei größten Wert auf die sichere Verteilung der chemischen Substanzen über das gesamte Werksgelände.

AS-Interface-Konzept bietet Vorteile

Der mit der gesamten Automatisierung beauftragte Systemintegrator DB Brooks arbeitet schon seit Jahren erfolgreich mit den sog. Safety-Integrated-Produkten der Siemens AG, um auf die speziellen Erfordernisse ihrer Kunden zugeschnittene Lösungen zu realisieren. So wurden auch bei der Steuerung für das Saatgutaufbereitungswerk die Vorteile des AS-Interface-Konzeptes genutzt und ein spezielles Steuergerät gebaut: das „Bayer Cropscience Pump Transfer System".

Damit die „Twin Vanguard"-Maschine entsprechend den genauen Qualitätsvorgaben das Saatgut aufbereitet, müssen Chemikalien aus Großbehältern in der ebenerdigen Fabrikhalle zum Standort der Maschine in einem oberen Stockwerk gepumpt werden. Die Verarbeitung von 24 Tonnen Saatgut pro Stunde im Stapelbetrieb in Intervallen von 15 Sekunden erfordert die exakte Verteilung von 36 Litern Flüssigkeit. Gerade im rauen industriellen Umfeld ist seitens der Automatisierungstechnik ein Höchstmaß an Sicherheit erforderlich. Ohne ein spezielles Sicherheitssystem ist das Risiko einer nachhaltigen Schädigung des gesamten Werkes z.B. auf Grund einer Fehlfunktion der Pumpenanlage zu hoch, die Auswirkungen auf die Umwelt könnten katastrophal sein.

Die Steuerung der Flüssigkeitsströme erforderte ein Informationssystem, das alle Container sicher verbindet und exakt steuert, wann wie viel Flüssigkeit aus den einzelnen Zwischengroßbehältern zur Aufbereitungsmaschine gepumpt werden soll.

Alle Container wurden mit einer einzigen AS-Interface-Leitung mit seinen bekannten, „modularen Fähigkeiten" – im Gegensatz zur sternförmigen Mehrfachverkabelung – verbunden. Diese gelbe, zweiadrige Leitung ermöglicht auf den ebenfalls am Kabel hängenden Anzeigefeldern (Operator Panels) auch die grafische Darstellung, wie voll der jeweilige Container derzeit ist, und gibt die Informationen an eine speicherprogrammierbare Steuerung (SPS) SIMATIC S7-200. Die SPS sendet wiederum ihre Steuersignale zu den Pumpensteuerungen, die dann entweder die Flüssigkeit zu den Maschinen pumpen bzw. die Container auffüllen.

Einfach, effektiv und höchst zuverlässig

Produktionsleiter Jim Donald von Bayer Cropscience sagt dazu: „Chemikalien in einem großen Fertigungsgelände exakt dosiert zu verteilen, kann eine schwierige Sache sein. Deswegen nehmen wir das Thema Sicherheit sehr ernst, indem wird dafür die Einhaltung der höchsten Standards verlangen. Wir erkannten während der Planung, dass die Verwendung des AS-Interface-Systems von Siemens uns den größten Nutzen bringen würde. Abgesehen davon, dass es sich hierbei um eine einfache, effektive und höchst zuverlässige Lösung handelt, ist die Gefahr, bei der Installation einen Fehler zu machen wegen der Verwendung einer einzigen Leitung sehr klein. Die Kostenersparnis war ein weiterer Grund, dieses System zu verwenden – es wurden nicht nur die Verdrahtungs- und Installationskosten reduziert, sondern auch das Risiko von Fehlern bei der Erst- oder bei späteren Änderungsinstallationen."

Kaum Produktionsausfall

Dies hat sich voll bewahrheitet: Die Produktionsunterbrechungen am Wynnstay-Standort während der Installation des neuen Automatisierungssystems waren minimal. Ohne großen Zusatzaufwand konnten die Entwickler des Systemintegrators DB Brooks das AS-Interface testen, indem sie es im eigenen Betrieb schon vor der eigentlichen Installation am endgültigen Standort aufbauten. Die einfache Montage des Netzwerks reduzierte die Produktionsausfallzeit drastisch im Vergleich zu herkömmlichen Verkabelungsmethoden.

(aus VERFAHRENSTECHNIK 38 (2004) Nr.1-2)

10.7 AS-Interface vereinfacht Arbeitsschutz bei UPS

Von 120 Mitarbeitern werden im UPS-Zentrum Aachen täglich bis zu 20000 Pakete sortiert und umgeschlagen.

An den Entladepositionen und an vielen anderen Stellen in der 700 Meter langen Sortieranlage sind Not-Halt-Befehlsgerät zur Sicherheit der Mitarbeiter angebracht. ASIsafe ist die installierte Steuerungstechnik, die hier für Sicherheit sorgt.

50 Zusteller starten ihre Tour mit Ihren typisch braunen Lieferwagen von der UPS-Zentrale in Eschleiler bei Aachen.

Wenn die Uhr im UPS-Zentrum Aachen 4.30 Uhr schlägt, kommt Leben in die Paketsortieranlage in Eschweiler/Weisweiler.
Bis 8.00 Uhr erfolgt die Paketsortierung zu einem schier endlos wirkenden Band, wo Mitarbeiter für die 50 Zusteller mit ihren typisch braunen Lieferwagen alle Pakete nach System so schnell wie möglich einladen. Das reibungslose Sortieren ist also das A und O. Weil aber die Unternehmensphilosophie von UPS nicht nur auf Geschwindigkeit und Präzision ausgerichtet ist, sondern auch auf die Sicherheit der Mitarbeiter, setzen die Verantwortlichen in Eschweiler auf Sicherheitsschaltelemente aus dem Siemens-Programm ASIsafe, um die Sicherheit zusätzlich zu erhöhen. Statt der bisherigen, konventionellen Schalttechnik entschied man sich bei UPS, Not-Halt-Befehlsgeräte mit AS-Interface einzusetzen. AS-Interface ist immer dann vorteilhaft, wenn einfache I/O-Geräte von der Maschinensteuerung angesprochen werden sollen.

Mit der neuen AS-Interface-Version 2.1 können bis zu 62 Slaves an einem Netz betrieben werden. Besonders interessant für Logistiker ist diese Art der Signaltechnik deshalb, weil seit kurzem über Sicherheitsmonitore die notwendigen Sicherheitsschaltungen realisiert werden können, wie sie in Verteilzentren gefordert sind. Überall dort, wo Mitarbeiter in die Nähe bewegter Teile kommen können, befindet sich ein Not-Halt-Befehlsgerät. In Eschweiler sind es 26.

Die Vorzüge der AS-i Safety-Sicherheitstechnik haben die UPS-Spezialisten schnell erkannt, und daher einer Lösung mit speziellem Sicherheits-Bussystem samt zusätzlichen Bauteil-, Installations- und Wartungskosten eine Absage erteilt. Die angesprochenen Sicherheitsmonitore vom Typ 3RK1105 werden bei der UPS-Lösung direkt an den in Eschweiler eingesetzten SIMATIC S7-300 Controller angeschlossen.
Die Nachrüstung der Anlage dauerte etwa zwei Wochen und erfolgte parallel

26 Not-Halt-Taster von Siemens sind an Schlüsselstellen der Paketsortierung montiert und über AS-Intersafe miteinander verbunden

zum alten System, ohne dass die täglichen Sortierprozesse gestört wurden. Innerhalb eines Tages ging das neue Sicherheitsnetz – zwischen zwei Schichten – komplett in Betrieb.
Wie bei allen Signalübertragungssystemen müssen auch bei AS-Interface bestimmte Eckwerte eingehalten werden. Nach spätestens 100 Metern muss ein Repeater zwischengeschaltet werden. Pro AS-Interface-Strang dürfen maximal zwei Repeater angeschlossen sein.

Im UPS-Zentrum Aachen hat die Betriebstechnik eine ganz eigene Lösung für die Positionierung der Signalverstärker gefunden. Da der Leitrechner sehr zentral in der Sortieranlage positioniert ist, konnte eine vollkommen untypische Reihenfolge der Slave-Nummerierung gewählt werden. Der Trick: Von den bereits erwähnten vier Sicherheitsmonitoren für die 26 Not-Halt-Befehlsgeräte können die typisch gelben AS-Interface-Kabel sternförmig verzweigt werden. Das führt dazu, dass selbst bei einer riesigen Paketsortieranlage mit einer Ausdehnung von 700 Metern keine Entfernungsprobleme entstehen. Dieses Beispiel zeigt, dass nicht immer eine einzige AS-Interface-Ringleitung direkt von der Steuerung gelegt werden muss, sondern dass AS-Interface flexibel auf die vorhandene Anlagengestaltung appliziert werden kann.

Störungen einfach erkennen

Das Schöne an der Schaltungstechnik ist, dass sofort sichtbar wird, welcher Not-Halt-Taster ausgelöst hat. Dazu gibt es in der Steuerung noch eine zusätzliche optische Anzeige, die es den Betriebstechnikern in der Logistik-Zentrale erleichtert, Störungen zu lokalisieren. Des Weiteren haben die Betriebstechniker bei UPS ein Monitormodul im Schaltschrank vorgesehen. Das SIMATIC C7 621 AS-Interface vereint den AS-Interface-Master CP 342-2, eine SIMATIC-CPU der S7-300-Klasse und ein Bedienpanel OP3 in einem Gehäuse.

Sicherheit bis Kategorie 4

Sobald ein Not-Halt-Befehlsgerät betätigt wird, steht die gesamte Sortieranlage. Zuerst war in Eschweiler geplant, im Notfall nur die Förderstrecken im Umkreis von 15 Metern stillzulegen – die Entfernung, die von den Sicherheitsvorschriften gefordert ist. Allerdings haben die Planer sofort erkannt, dass damit fast alle Bänder stehen würden. Also hat man sich darauf geeinigt, innerhalb von Millisekunden alles abschalten zu können.

Mit AS-i Safety von Siemens können Anwendungen bis zur Kategorie 4 gemäß EN 954-1 ausgerüstet werden. Die geforderte sichere Kommunikation zwischen den sicheren Slaves und dem Sicherheitsmonitor wird durch eine zusätzliche Signalübertragung geschaffen. Der Sicherheitsmonitor „erwartet“ zyklisch von jedem Sicherheits-Slave ein vier Bit langes Telegramm, das sich nach einem definierten Algorithmus kontinuierlich ändert. Trifft nun durch eine Störung das erwartete Telegramm nicht ein oder wird das für den Alarmfall reservierte Telegramm 0-0-0-0 empfangen, schaltet der Sicherheitsmonitor nach maximal 40 ms über seine zweikanalig ausgeführten Freischaltkreise die sicherheitsgerichteten Ausgänge ab.

Neben den im UPS-Zentrum Aachen neu installierten Not-Halt-Befehlsgerät lassen sich natürlich auch alle anderen typischen I/Os wie Magnetschalter, Taster, Laserscanner oder Lichtschranken, -gitter und -vorhänge in der sicheren AS-Interface-Technik ausführen.

Siemens bietet hierzu sein komplettes Programm an Sicherheitsgeräten von „Safety Intergrated“ an. Mit Hilfe einer einfachen AS-Interface-Konfigurationssoftware werden solche Geräte den Sicherheitsmonitoren zugeordnet.

Flexibel erweiterbar

Mit Blick auf die schrittweise Modernisierung von Anlagen haben sich die Betriebstechniker für die nächste Umrüstaktion „AS-i Safety“ in ihr Pflichtenheft notiert.

Denn nach ihren Aussagen ist die Flexibilität des Systems unglaublich hoch. Zumal nun nicht mehr nur einfache Signale, sondern mittlerweile auch ganze Datenpakete übertragen werden können. Damit schließt sich eine wichtige Diagnoselücke bei AS-Interface.

Logistikzentren profitieren von der AS-Interface-Technik doppelt. Denn durch die einfache Anschlusstechnik über Durchkontaktierungen lassen sich sämtliche

Schaltgeräte schnell an- und abklemmen. Dabei braucht der Techniker keinen Schraubenzieher mehr für die Leitungen. Bevor ein AS-Interface-Gerät abgenommen wird, bringt es der Techniker mit einem Knopfdruck in eine Servicefunktion. Das neue Gerät wird dann einfach eingesetzt, ohne dass es programmiert werden muss. Denn in einem AS-Interface-Strang werden die einzelnen „Platznummern“ in der Anlage gespeichert. Das neue Endgerät meldet der Techniker per erneutem Knopfdruck dann wieder beim Host-Rechner an. Dafür sind auch keine speziell ausgebildeten Fachleute notwendig. Das ist deshalb so wesentlich, weil gerade Logistikzentren meist sehr weit verzweigt und die Wege lang sind.

Auch sonst ist die Technik sehr anwenderfreundlich. Nach den Erfahrungen der Verantwortlichen bei UPS lassen sich Störungen schnell beheben und auch bei der Inbetriebnahme geht es ruck, zuck. Jeder Mitarbeiter ist sehr schnell mit den AS-Interface-Geräten vertraut. Damit wird wertvolle Zeit gespart. Und das ist schließlich die zentrale Aufgabe der Logistik.

Niederlassungsleiter des UPS-Zentrums Aachen Stefan Höfer (re.) und Siemens-Berater Heinz Czichy freuen sich über die neue und einfache Sicherheitslösung mit AS-i Safety. Durch den zentral gelegenen Schaltschrank konnte eine besondere AS-Interface-Verkabelung realisiert werden

10.8 CROWN Vourles – Verpackungsindustrie sicher mit Safety Motorstarter Solution PROFIsafe

Nach einer normgerechten Anpassung der Produktionslinie 22 der Verpackungsfirma „Crown Speciality Packaging France", läuft diese nun mit PROFIsafe. Der Zentralprozessor 416F des Automaten S7-400 verwaltet gleichzeitig die Standard- und die Sicherheits-Ein- und Ausgänge. Die Steuerfunktionen werden von Touchscreens die auf dem MPI-Bus angeschlossen sind, unterstützt. Die angewandte Technologie ermöglichte es, gerade durch den Einbau von Safety Motorstartern Solution PROFIsafe, die Prüf- und Bearbeitungszeit zu halbieren.

CROWN Holdings in Vourles/Lyon in Frankreich ist einer der Marktführer in der Verpackungsindustrie. Die Firma ist Hersteller von spezifischen Metallverpackungen. Dazu zählen Getränkedosen, Konservendosen und Spezialverpackungen für große Marken (z.B. Bonduelle, Coca-Cola u.a.) in "kleinen Mengen", d.h. max. 25 Millionen Stück pro Produktionslinie und Jahr.

Hergestellt werden „vor allem sogenannte dreiteilige Dosen", erzählt Gilles Guerrin, der Technik-Verantwortliche des Standortes: „Jede setzt sich zusammen aus einem gerundeten oder geschweißten Rumpf, einem tiefgezogenen Deckel, auf dem der Verschluss angebracht wird und einem ebenfalls tiefgezogenen Boden."

Auf der Linie 22 werden industrielle Eimer mit einem Durchmesser von 220 mm und einem Fassungsvermögen von 5 bzw. 6 Litern hergestellt. „Die stündliche Produktion übersteigt 2500 Stück, es wurde also erforderlich, die Linie an das Dekret 9340 der französischen Norm für Maschinensicherheit anzupassen. Ziel war auch, die Produktivität zu erhöhen, indem wir die Linie richtig einstellen und letztlich weniger Personal an der Linie binden."

Außerdem bringt die automatisierte Produktion der "Trichtereimer" den Einbau einer neuen Maschine für das Einfassen der Ringe mit sich und ersetzt die zwei manuellen Maschinen, die bis zu diesem Zeitpunkt von vier Personen bedient wurden.

Vierzehn Maschinen in Serie

Die Linie 22 besteht aus 14 Maschinen in Serie, die mit Stahlblättern versorgt werden:

- Die Schweißmaschine rollt das ebene Metallblatt, bevor der so geformte Zylinder zusammengeschweißt wird.
- Der hydraulische Expander verleiht der Röhre die Form eines Kegelstumpfes.

- Die Formmaschine verformt den oberen Teil dieses Kegelstumpfes so, dass er obere Teile aufnehmen kann.
- Die Ringmaschine vollendet diese Operation. Gleichzeitig wird im Rumpf ein Ring eingesetzt, um die zu tiefe Verschachtelung der Eimer zu vermeiden. So kann man sie später problemlos trennen.
- Jeder Eimer wird umgedreht, bevor er die folgenden Maschinen durchläuft: die Einfassmaschine, dann die Dosenverschlussmaschine. Der Durchmesser wird reduziert, während der Rand so gebogen wird, dass man den Boden auf den Rumpf schweißen kann.
- Der Eimer wird erneut umgedreht, bevor die Kehlmaschine das Oberteil des Eimers vorbereitet.
- Die Schweißmaschine setzt auf beiden Seiten des Rumpfes Scheiben für die Henkelhalterung ein. Die Henkel werden durch die Schwerkraft mit Hilfe einer zentrifugalen Schleudertrommel verteilt und genau an der Schweißnaht positioniert.
- Die Lackiermaschine stellt den Schutz der geschweißten Elemente sicher.
- Der Tunnel dient der Trocknung des aufgetragenen Lackes.
- Die doppelte Ringverschlussmaschine wurde in Lycée Lamache erneuert.
- Das Bügelinstallationsgerät bringt den Henkel auf den Scheiben an.
- Die hergestellten Eimer werden schließlich automatisch gestapelt.

Die normgerechte Anpassung der Eimer-Produktionslinie

Vierzehn Maschinen mussten also angepasst werden. Notwendigerweise mit sehr kurzen Interventionszeiten, um die zu lange Stilllegung der Produktion und damit Wartezeiten für den Kunden zu vermeiden.

Die Vorarbeit begann im Mai 2003. Die erste Maschine wurde im darauffolgenden September normgerecht angepasst. Nach drei weiteren Eingriffen waren alle Bestandteile der Linie eingefügt.

Diese Anpassung zeigt in folgenden Punkten Auswirkungen auf die Sicherheit:

1. Schutz der Maschinen: Ersatz der nicht geregelten Gitter durch Lichtvorhänge und der Einbau von festen Schutzgittern auf der Rückseite.

2. Die konventionellen Steuerpulte wurden durch SIMATIC Touch Panels mit zwei Not-Halt-Befehlsgeräten ersetzt: Der eine Not-Halt für den lokalen Halt der Maschine, der andere für den Halt der gesamten Linie.

3. Die normgerechte Umsetzung der pneumatischen Verteilung hat das Auswechseln der Verteiler und der Ventilversorgungsblocks sowie die Regelung der pneumatischen Versorgung vorausgesetzt.

Außerdem erfolgte die technische Anpassung auch durch folgende Aktionen:

1. An den Gehäusen mit den mechanischen, schwer einstellbaren Nockenschaltwerken wurden Geber eingebaut, deren Einstellung direkt auf dem OP mit einer viel höheren Genauigkeit (auf das Grad genau) geändert werden kann.

2. Schließlich wurden die Schaltschränke erneuert, die verkabelten Sicherheitsrelais wurden durch ein automatisiertes Sicherheitssystem SIMATIC ersetzt: ein Zentralschaltschrank mit der Steuerung S7-416F ist an andere Schaltschränke mit der Peripherie ET 200S angeschlossen.

„Wir haben mit Siemens und unserem Installateur begonnen, die notwendige Automatisierungsarchitektur zu untersuchen“, erläutert Gilles Guerrin. „Wir arbeiten seit 25 Jahren mit SNEF (einem Spezialisten zur Automatisierung industrieller Vorgänge) zusammen, sowohl in Frankreich als auch im Ausland“. Gilles Guerrin: „Siemens war der einzige Hersteller von Automatisierungstechnik, der einen Sicherheits-SPS mit Standardfeldbus Kommunikation realisiert."

Die Linie wird heute von drei Netzen durchzogen, die die verschiedenen Maschinen verbinden:

1. Ein Stromnetz durchläuft die ganze Linie. Der Zentralschaltschrank ist an jeden maschinennahen Verteilerschrank angeschlossen.

2. An das MPI-Netz (196 Kbaud) werden 10 Panels TP170B angeschlossen. Sie ersetzen alle konventionellen Knöpfe bis auf die Not-Halt-Befehlsgeräte.

3. Das Netz PROFIBUS DP mit dem Profil PROFIsafe verbindet die Produktionsanlagen mit dem Steuerung SIMATIC S7-416F. Über dieses Netz werden Sicherheitstelegramme mit Standardteilnehmern ausgetauscht. Der SPS ist so mit 19 DP-Slaves verbunden, und zwar mit 13 ET 200S Peripherie Stationen, 5 Umrichtern und 2 pneumatischen Blöcken.

Man zählt außerdem insgesamt 248 Eingänge und 124 Ausgänge, 64 Sicherheitseingänge, 64 Sicherheitsausgänge, 43 sichere Motorstarter Failsafe und 7 SSI-Modulen für den Anschluss der Positionierungsgeber.

Was das Sicherheitsnetz betrifft, betont Gilles Guerrin, „hat PROFIsafe den Vorteil, dass es die Sicherheitskommunikation auf einem Standard PROFIBUS DP ermöglicht". Und somit auch den höchsten Kommunikationsstandard gemäß der Sicherheitsnorm IEC 61508. Die Standard Kommunikation und die sicherheitsgerichtete Kommunikation können auf ein und derselben Sammelleitung verbunden werden.

Die Wahl des ET 200S Peripheriesystems mit ihrer Modularität hat sich auch aufgrund der Unterstützung der Sicherheitsfunktion und des damit erreichten Verdrahtungsgewinns durchgesetzt. „An den ET 200S-Stationen konnten wir die Failsafe-Motorstarter einbauen. Sie ermöglichen es, selektive Sicherheitsabschaltungen in aller Einfachheit durchzuführen, und sie entsprechen den Sicherheitsanforderungen der Kategorie 4 nach EN 954-1. Zusätzlicher Vorteil: redundanter Netzschutz ohne weitere Verkabelung".

Doppelte Geschwindigkeit, halber Preis

"Während wir früher eine Art Hardware-Intelligenz hatten, die mit einer Art Software-Intelligenz verbunden war, ist heutzutage alles soft ...im SPS"

Für Gilles Guerrin hat dieser Umbruch weitreichende Folgen. Verglichen mit einem konventionellen Schema, bei dem die Terminalklemme und die Sicherheitsrelais verdrahtet werden mussten, wurde, dank der elektronischen Verwaltung der klassischen Ein- und Ausgänge sowie der Sicherheitsein- und -ausgänge und mit dem Anschluss an das Netz der Motorstarter, die Prüfzeit halbiert. Die Verdrahtungszeit selbst wurde ebenfalls halbiert, da die Sicherheitsfunktionen nicht mehr verkabelt werden und die Motorstarter über PROFIsafe kommunizieren. Schließlich ermöglichen es die Umgruppierung der Systemintelligenz, sowie die Anordnung der Gesamtheit der Informationen am gleichen Ort der programmierbaren Steuerung, die Inbetriebnahme der Linie zu vereinfachen.

10.9 Mehr Sicherheit in der Automobilindustrie

Seit Ende 1998 ist die neue flexible Fertigungslinie im Renault-Werk von Cleon in Nordfrankreich im Einsatz. Pro Woche fertigen dort 40 Maschinen rund um die Uhr 5000 Zylinderköpfe. Jede dieser Maschinen ist mit einer SINUMERIK 840D mit Safety Integrated ausgestattet. Wir fragten den Leiter der Fertigungslinie, Patrick Renault, nach seinen bisherigen Erfahrungen mit der integrierten Sicherheitstechnik von Siemens.

Herr Renault, seit September 1998 läuft die neue Fertigungslinie. Woraus besteht die Linie und was produziert sie?

Patrick Renault: Neben insgesamt 40 Maschinen sind noch 13 Ladeportale, Einlauf und Auslauf sowie die Montageeinheiten, die Messstationen und die Beschriftungseinheiten im Einsatz. Die Linie arbeitet rund um die Uhr – einzige Ausnahme sind sechs Stunden am Sonntagmorgen. Produziert werden verschiedene Varianten von Zylinderköpfen für Motoren von 1,4 bis 2,2 Liter Hubraum.

Alle 40 Maschinen sind mit Safety Integrated in Verbindung mit einer SINUMERIK 840D ausgerüstet. Was hat Sie zu der Entscheidung bewogen, Safety Integrated einzusetzen?

Patrick Renault: Der Einsatz von Safety Integrated ist zunächst vom Maschinenbauer (Firma Grob) vorgeschlagen und realisiert worden. Inzwischen sind wir recht froh über diese damalige Entscheidung. Denn da die Maschinen mit großer Geschwindigkeit arbeiten – 60 bis 70 Meter pro Minute auf den Bearbeitungszentren und 120 Meter pro Minute bei den Ladeportalen –, ist es unerlässlich, ein Maximum an Sicherheit zu bieten. Und das können wir mit Safety Integrated.

GROB-Bearbeitungszentrum in der Fertigungslinie

Leiter der Fertigungslinie Patrick Renault

Welche weiteren Vorteile bringt die integrierte Sicherheit im Vergleich zur konventionellen Sicherheitstechnik?

Patrick Renault: Zunächst hat sie viel kürzere Reaktionszeiten, da sie in die numerische Steuerung der SINUMERIK 840D integriert ist. Außerdem ist mit Safety Integrated die sichere reduzierte Geschwindigkeit möglich. Sie erlaubt uns, bei geöffneten Schutztüren und laufender Maschine einzugreifen – und das mit 100%-Sicherheit. Durch diese Möglichkeit brauchen die Antriebe nicht mehr von der Spannung getrennt zu werden. Dies bedeutet eine verlängerte Lebensdauer der Antriebe – Sie wissen ja, dass häufiges An- und Abschalten der Zwischenkreisspannung die Lebensdauer beeinflusst.

Welche Kriterien haben Sie veranlasst, die integrierte Sicherheit auf allen Ihren Produktionslinien als Standard einzusetzen?

Patrick Renault: Das Ziel von Renault heißt klar: Wir wollen ausschließlich Maschinen einsetzen, die die Kategorie 3 der Sicherheitsnorm EN 954-1einhalten und mit schnellen Reaktionszeiten ein hohes Sicherheitsniveau erreichen. Diese Anforderungen werden mit Safety Integrated erfüllt.

Ist das Bedienpersonal mit der integrierten Sicherheit zufrieden?

Patrick Renault: Es ist klar, dass die Möglichkeit, bei geöffneter Tür während der Service-Zeiten oder beim Einrichten der Portale von Hand an der Maschine zu hantieren, Vertrauen schafft. Der Einsatz von Safety Integrated ist außerdem recht transparent, d.h., es ergeben sich keine Probleme während der Produktion. Und obwohl die Geschwindigkeiten der jetzigen Fertigungslinie erheblich höher sind, hat das Bedienpersonal verstanden, dass Safety Integrated ihm mehr Sicherheit bietet.

Herr Renault, wir danken Ihnen für das Gespräch.

10.10 Neuer Standard für Werkzeugmaschinen

Das schwäbische Unternehmen Alfing Kessler Sondermaschinen GmbH, aus Aalen, setzt schon seit einiger Zeit auf flexible Fertigungsanlagen. Der neueste Baustein zur Leichtmetallbearbeitung ist der ALFING 2-Spindler, die u.a. bei VW Sachsen in Chemnitz eingesetzt werden. Eines der besonderen Kennzeichen dieser Maschinen ist die integrierte Sicherheitstechnik von Siemens.

Statt starrer Transferstraßen flexible Fertigungsanlagen, statt Sondermaschinen standardisierte Baueinheiten – Modularität ist in modernen Fertigungsanlagen immer mehr gefragt. Standardisierte Baueinheiten erleichtern nicht nur die Wartung und erhöhen dadurch die Verfügbarkeit. Sie bilden auch die Voraussetzung dafür, fertige Anlagen zu erweitern und zu verändern – auch und besonders durch neue Maschinenbausteine, wie etwa den 2-Spindler von Alfing Kessler für flexible Fertigungsanlagen zur Leichtmetallbearbeitung.

Gerade im Fahrzeugbau führt die Leichtbauweise zu immer mehr Einsatz von Leichtmetall. Somit wundert es auch nicht, dass die ALFING 2-Spindler in der Automobilfertigung von VW Sachsen zur Bearbeitung von aus Aluminium gegossenen Zylinderkopfhauben (Aluminium-Druckgussteil) eingesetzt werden.

Minimale Nebenzeiten

Die beiden getrennt angetriebenen Arbeitsspindeln arbeiten beim ALFING 2-Spindler unabhängig voneinander. Während die eine Spindel das Werkstück bearbeitet, holt die zweite Spindel im Pick-up-Verfahren ihr nächstes Werkzeug aus dem jeder Spindel zugeordneten Magazin (mit einer Kapazität von 48 Werkzeugen). Die zweite Spindel wird anschließend direkt auf Nenndrehzahl beschleunigt. Dadurch befindet sich das gerade eingewechselte Werkzeug schon im rotierenden Zustand und kann sehr schnell seine Arbeit aufnehmen. Dies geschieht in höchstens einer Sekunde, nachdem die erste Spindel fertig ist und ihrerseits den Werkzeugwechsel im Magazin vollzieht. Die wirksamen Nebenzeiten reduzieren sich so auf den schnellen Tausch im Einsatz der beiden Spindeln. Und das erhöht drastisch die Produktivität: In nur ca. 165 Sekunden ist eine Zylinderkopfhaube fertig bearbeitet. Das Konstruktionsprinzip des 2-Spindlers basiert auf leichten, beweglichen und schweren, ortsfesten Massen. Nur so lassen sich die geforderte Schnelligkeit und Stabilität erreichen. Die Achsbewegungen sind verteilt: Die Y- und Z-Bewegung führt das Werkzeug, die X-Bewegung hingegen das Werkstück. Der Arbeitsbereich erstreckt sich über 880 x 630 x 500 mm (X, Y, Z).

Bedienkonzept mit SINUMERIK, Safety Integrated

Erstmals mit SINUMERIK Safety Integrated

Gesteuert wird die Maschine von einer SINUMERIK 840D und SIMODRIVE 611D – für den Einsatz im Fertigungswerk von VW Sachsen erstmals mit Safety Integrated, inklusive sicherer programmierbarer Logik, (SPL) ausgerüstet.

„Bei derartig hochdynamischen Maschinen, mit Beschleunigungen von über 10 m/s2, ist es unserer Meinung nach nicht mehr zu verantworten, diese ohne Safety-Funktionen zu liefern", erläutert Willi Diemer, der Leiter der Elektrokonstruktion, seine Entscheidung für SINUMERIK mit Safety Integrated. Und warum integrierte Sicherheit? „Nur mit integrierter Sicherheitstechnik

lässt sich die reduzierte Geschwindigkeit sicher überwachen", erklärt Diemer. „Geschieht dies nicht, wird die Geschwindigkeit zwar über die Software reduziert, aber sobald die Maschine einen Fehler hat, würde sie ohne Safety-Funktion einfach losschießen. Was dies bedeuten kann, ist klar."

Weniger Relais bedeuten weniger Ausfälle

Sicherheitstechnik ist auch vonnöten, um die Antriebe bei offener Schutztür mit sicher reduzierter Geschwindigkeit zu fahren, wenn z. B. Einrichtarbeiten vorzunehmen sind. Während konventionelle Sicherheitstechnik nur Leistung abschalten kann, setzt Safety Integrated im Fehlerfall die Maschine schneller und sicherer still. Eine Leistungsabschaltung ist nicht mehr zwingend erforderlich. Nur der Antrieb, der wirklich unkontrollierbar geworden ist, wird automatisch von der Energiezufuhr getrennt. Das bringt den entscheidenden Augenblick mehr an Sicherheit für den Bediener und schont Maschine und Prozess. „Den Startschuss bei Alfing für diese Technik hat die sichere programmierbare Logik gebracht", berichtet Willi Diemer. „Denn besonders mit ihr lassen sich konventionelle Schaltgeräte einsparen." Das hat nicht nur Preisvorteile. Eine mit Safety Integrated und SPL ausgerüstete Maschine kann nahezu preisneutral angeboten werden. (Eine Option stellt jedoch das Fahren der Maschine über Zustimmtaster dar.) Außerdem bedeuten weniger Relais auch weniger Ausfälle und dadurch höhere Sicherheit und eine höhere Verfügbarkeit der Maschine. Wenn nämlich ein wichtiges Relais, beispielsweise das, welches die Impuls- oder Reglerfreigabe der Antriebe schaltet, ausfällt, dann kann die Maschine nicht mehr kontrolliert bremsen, der Motor trudelt aus – und ein Crash der Maschine wäre nicht mehr auszuschließen.

Überzeugendes Konzept

Für den Kunden von VW Sachsen war Safety Integrated mit SPL eine neue Technik, die man zunächst prüfen wollte. Alfing Kessler hat die nach den Siemens-Spezifikationen projektierte und anschließend so aufgebaute Maschine samt den Safety-Funktionen den Verantwortlichen von VW Sachsen, VW-Produktionsplanung und Vertretern der Berufsgenossenschaft Mainz (Eisen Metall II) überzeugend präsentieren können. Besondere Beachtung fand die – gemäß Siemens-Spezifikation – durchgängig 2-kanalige Auslegung aller Sicherheitskomponenten, wie z. B. für Schutztüren und Not-Aus. Selbst die Querschlussüberwachung der beiden Sicherheitskanäle wurde bei diesen Maschinen über das „4-Klemmen-Konzept" realisiert.

Wichtig war für VW auch, die Maschine bei „offener Schutztür" zu fahren. Mit Safety Integrated lässt sich das Bedienkonzept der Maschine optimal auf die Bedürfnisse des Bedieners und die Prozess-Anforderungen abstimmen, was das Einrichten der Maschine enorm erleichtert. Die heute leider immer noch üblichen Manipulationen werden somit schon im Ansatz verhindert. Jetzt werden weitere Maschinen nach demselben Konzept für VW Kassel, SKODA-Auto und DaimlerChrysler gebaut.

Für Willi Diemer ist klar: „Bei unseren hochdynamischen Maschinen möchten wir nicht mehr auf integrierte Sicherheitstechnik von Siemens verzichten."

10.11 Sicherheit bei der Produktprüfung von Arbeitsschutztechnik

Moderner Arbeitsschutz an Maschinen ist ein gutes Beispiel für den Einzug neuer Technologien in die heutige Arbeitswelt. Sie sorgt nicht nur dafür, dass Menschen und Maschinen sicher zusammenarbeiten können, sondern ermöglicht darüber hinaus auch einen hohen wirtschaftlichen Nutzen – früher ein nicht aufzulösender Widerspruch.

Zusammenfassung

Zum Schutz von Personen in Gefahrbereichen an Maschinen finden sich zunehmend Sicherheitsprodukte wie Laserscanner und Kamerasysteme, die zu den „berührungslos wirkenden Schutzeinrichtungen" (BWS) der Arbeitsschutztechnik gehören. Zu deren Untersuchung und Prüfung nutzt das Berufsgenossenschaftliche Institut für Arbeitsschutz – BIA bereits seit einiger Zeit eine Prüfanlage mit Linearachsen in einem offenen Aufbau. Um die zeitlich aufwändigen Prüfreihen noch schneller, einfacher und damit insgesamt effizienter durchführen zu können, wurde die Prüfanlage nun mit dem „neuesten Stand der Technik" aufgerüstet. Dazu zählen die integrierten Sicherheitsfunktionen der Siemens CNC-Steuerung SINUMERIK840D, eine Vernetzung aller sicherheitsgerichteter Anlagenteile über den Feldbus Profibus mit PROFIsafe-Profil und vier neue Laserscanner Siguard LS-4 PROFIsafe für die Absicherung der Schutzfelder.

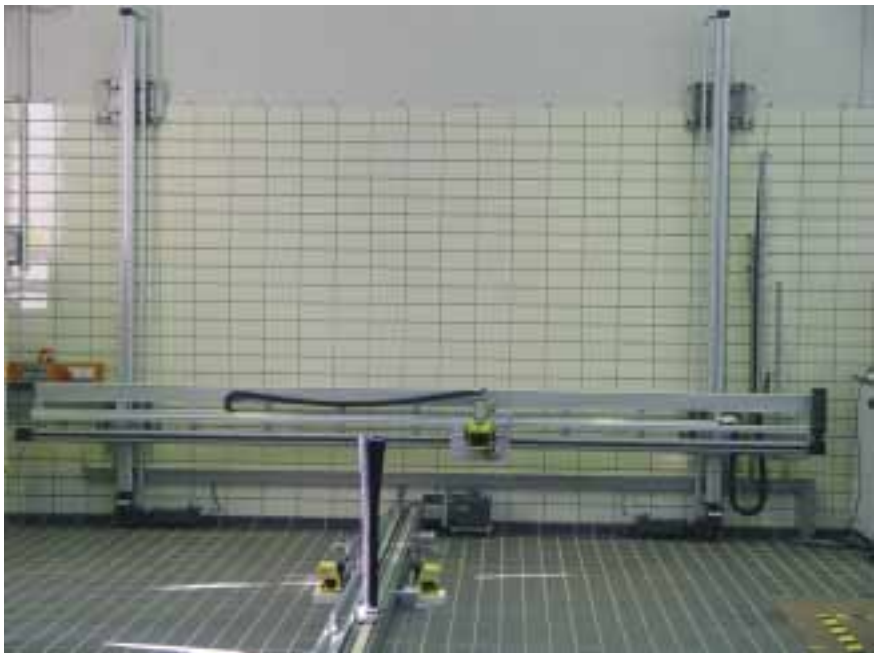


Bild 10/1
Die modernisierte und automatisierte BIA-Prüfanlage für und mit Sicherheitstechnik der neuesten Generation macht die gesetzlich vorgegebenen Produktprüfungen effizienter – und bietet den Prüfern selbst „Rund-um-Sicherheit"

Produktprüfung und -zertifizierung beim BIA

Das Berufsgenossenschaftliche Institut für Arbeitsschutz ist ein Forschungs- und Prüfinstitut der gewerblichen Berufsgenossenschaften (BG). Das BIA unterstützt die gewerblichen Berufsgenossenschaften und deren Institutionen schwerpunktmäßig bei naturwissenschaftlich-technischen Fragestellungen im Arbeits- und Gesundheitsschutz durch

- Forschung, Entwicklung und Untersuchung
- Prüfung von Produkten und Stoffproben
- Betriebliche Messungen und Beratungen
- Mitwirkung in der Normung und Regelsetzung
- Bereitstellung von Fachinformationen und Expertenwissen.

Darüber hinaus wird das BIA europaweit tätig für Hersteller und Firmen im Rahmen der

- Produktprüfung und -zertifizierung
- Zertifizierung von Qualitätsmanagementsystemen.

Für neuartige Schutzeinrichtungen führt das BIA Grundlagenuntersuchungen/Forschungsarbeiten durch, entwickelt Prüfverfahren und arbeitet in der Normung, berät bei Produktentwicklung und Einsatz und führt als notifizierte Prüfstelle Produktprüfungen und -zertifizierungen durch. Zurzeit besteht für diese Sicherheitsprodukte eine Prüfpflicht.

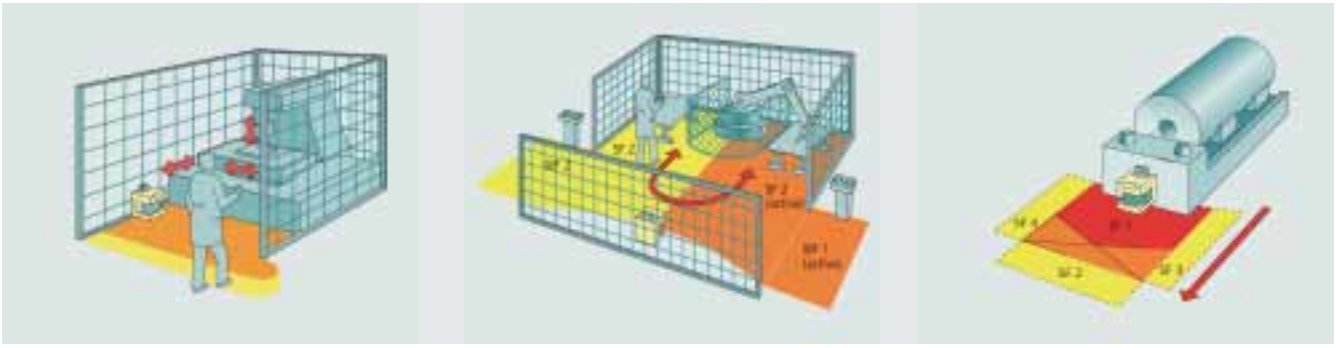


Bild 10/2
Vielfältige Anwendungsbereiche von Laserscannern

Teilautomatisierte Produktprüfung – z.B. von Laserscannern

Laserscanner sind optische Distanz-Sensoren und werden in unterschiedlichen Anwendungen als Personenschutzsysteme eingesetzt:

- Gefahrenabsicherung an stationären Maschinen und Robotern
- Fahrwegüberwachung bei fahrerlosen Transportsystemen

Hierzu müssen sie Personen vorausschauend in Gefahrbereichen wie z.B. dem Fahrweg direkt vor einem fahrerlosen Flurförderzeug erkennen und ein entsprechendes sicheres Signal ausgeben, mit dem die jeweilige gefahrbringende Bewegung abgewendet werden kann. So wird das Flurförderzeug beispielsweise über dessen Antrieb und Bremse in den Stillstand abgebremst und solange dort gehalten, wie sich Personen im Gefahrbereich aufhalten.

Das sichere Erkennen einer Person – unter allen Einsatzbedingungen und sogar im Falle eines Fehlers in seiner Optik, Mechanik oder Elektronik – ist dabei eine maßgebliche Eigenschaft der Laserscanner. Im Rahmen der Produktzertifizierung beim BIA sind die Prüfung aller Sensoreigenschaften und die Vermessung der Überwachungsbereiche, den so genannten Schutzfeldern, ein wichtiger Bestandteil. Einzelprüfungen zum Detektionsvermögen, der Schutzfeldgeometrie, Mess- und Abbildungsgenauigkeit, Auflösung, Reaktionszeit und der Funktionsfähigkeit bei Umgebungseinflüssen wie Fremdlicht machen diese Prüfung insgesamt recht umfangreich und zeitintensiv. Erst mit Hilfe einer Prüfanlage sind diese Aufgaben weitgehend automatisiert und insbesondere mit einer hohen Präzision und Reproduzierbarkeit durchführbar.

Automatisierte Prüfanlage

Die größte „Hilfsarbeit", die eine Prüfanlage zu den oben aufgezählten Untersuchungen von berührungslos wirkenden Schutzeinrichtungen (BWS) beitragen kann, ist das exakte Positionieren und Verfahren von Referenzzielen, sog. Prüfkörpern, die jeweils mit wohl definierten Eigenschaften Körperteile von Personen nachbilden. Hier kommen keine Probanden oder Schaufensterpuppen zum Einsatz, weil Prüfkörper ein weit höheres Maß an Reproduzierbarkeit der Messergebnisse erzielen und Kennwerte aufweisen müssen, die eine „schlechte-Bedingungen"-Charakteristik für die Personenerkennung nachvollziehen. Die Prüfanlage im BIA stellt mittels Linearachsen dafür zwischen dem Prüfling – also der zu bewertenden Schutzeinrichtung – und dem Prüfkörper ein dreidimensionales Koordinatensystem her. In den Bildern 1 und 3 erkennt man den Prüfling als gelbes „Kästchen" auf dem Läufer des X-/Y-Portals und den Prüfkörper als Zylinder auf dem Läufer der Z-Achse.

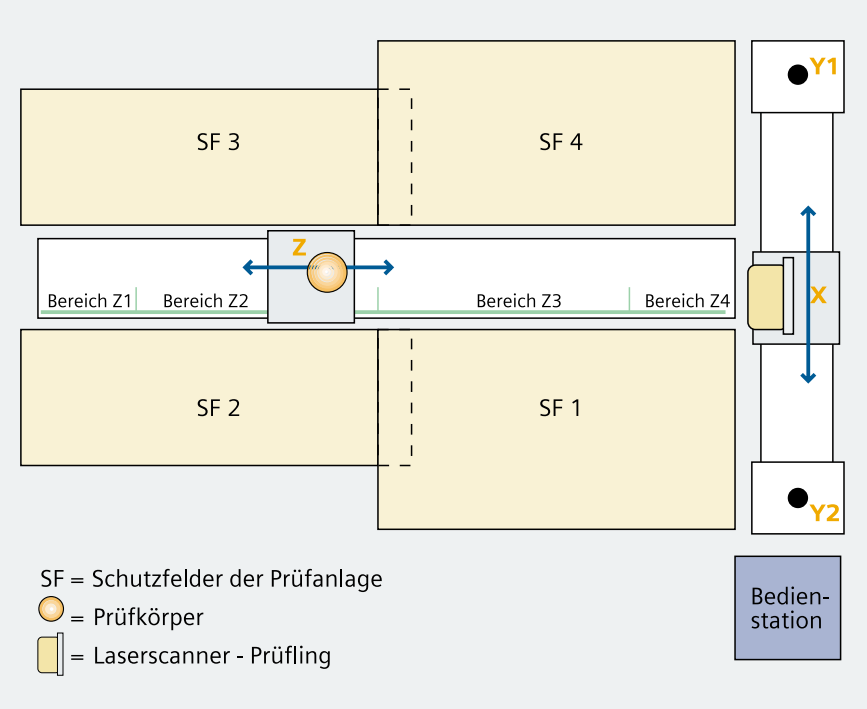


Bild 10/3
Schematische Achs-Schutzfelddarstellung (Draufsicht)

Bei der Vermessung von Schutzfeldern hat die Prüfanlage nun die Aufgabe, den Prüfkörper in beliebig feinen Rasterschritten zu positionieren und den Prüfling dort jeweils abzufragen, ob er den Prüfkörper erkennt. Die Vielzahl von Ja-/Nein-Messdaten lassen sich zu einem zwei- bzw. dreidimensionalen Ergebnisbild über die Schutzfeldgeometrie und evt. vorhandener Lücken zusammenstellen. Soll die Reaktionszeit einer Schutzeinrichtung gemessen werden, verfährt die Prüfanlage den Prüfkörper mit variabler Geschwindigkeit in das Schutzfeld des Prüflings und wertet den zeitlichen Verzug bis zu seinen Ausgangsschaltsignalen aus. Dies simuliert z.B. auch eine reale Annäherung eines Fahrzeugs auf eine Person. Neben den (vier) Achsen ist also noch eine „intelligente" Steuerung notwendig, die all diese Prüfszenarien koordiniert „abwickelt", eine Bedieneroberfläche für ein Prüfprogramm enthält, mit dem die Prüfaufgabe, der Prüfablauf und Gerätedaten konfiguriert werden können und einen Programmbereich anbietet, in dem die gesammelten Messdaten des Prüflings angezeigt und/oder ausgewertet werden.

Hinzu kommt: Die Prüfanlage hat einen offenen, zugänglichen Aufbau. Und was für millimetergenaue Positionierbewegungen noch vollkommen harmlos aussieht, ändert sich bei dynamischen Prüfprogrammen. Entweder der Prüfkörper oder der Prüfling „flitzt" hierbei mit hoher Geschwindigkeit durch den (Prüf-)Raum. *Anmerkung: noch ein Grund mehr, nicht mit Probanden zu arbeiten!* „Safety first" lautete im BIA natürlich die Maxime und als Ergebnis einer Gefährdungsanalyse wurden wie bei industrieüblichen Bereichsabsicherungen an Maschinen auch die verletzungsgefährdeten Bereiche der Achsen abgesichert – wen wundert´s: mit Laserscannern.

Laserscanner der neuesten Generation

In der Prüfanlage sorgen die vier Laserscanner Siguard LS-4 PROFIsafe mit den Schutzfeldern SF1 bis SF4 (in Bild 10/3 nur vereinfacht dargestellt) in den Achsverfahrbereichen für einen perfekten Personenschutz. Über eine integrierte Schnittstelle ist der Laserscanner direkt an den Profibus mit PROFIsafe-Profil angebunden. Die Zertifizierung des für Anwendungen bis zur Kategorie 3 nach EN 954-1 geeigneten Laserscanners erfolgte übrigens auch beim BIA, so dass der ehemalige Prüfling nun an der Prüfanlage seinen Dienst zum Nutzen der Sicherheit verrichtet.

Bild 10/4
Neuer Laserscanner SIGUARD LS-4 PROFIsafe – Einfache, sichere Installation durch integrierte Profibus-Schnittstelle

Einfache Installation durch direkten Anschluss an den Profibus

Die Wahl für die Verbindungstechnik zwischen den Laserscannern und der sicherheitsgerichteten Anlagensteuerung – der SINUMERIK 840D – fiel auf den Profibus mit PROFIsafe-Profil. Er stellt sowohl die direkte Verbindung zu den Laserscannern her als auch zu allen anderen sicherheitsgerichteten Anlagenteilen, wie z.B. den Not-Halt-Tastern, Betriebsartenschlüsselschaltern und den Haltebremsen. Sie sind direkt, ohne zusätzlichen Geräteaufwand und damit kostensparend an die fehlersicheren Ein-/Ausgangsmodule SIMATIC ET 200S angeschlossen – alles mit dem großen Vorteil einer Reduzierung der Aufwände für Engineering und Installation.

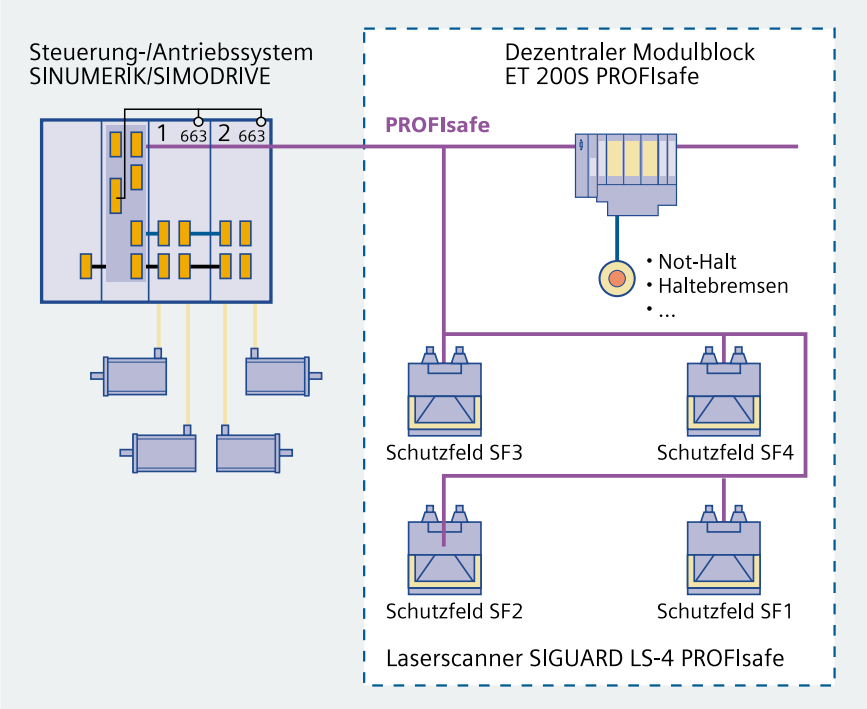


Bild 10/5
Profibus mit PROFIsafe-Profil für die Vernetzung aller Sicherheitskomponenten führt zu einer einfachen Anlageninstallation

Zusätzliche Sicherheit in Steuerungs-/Antriebsystem integriert

Schon im Jahre 1996 wurde die Prüfanlage mit einer CNC-Steuerung automatisiert. Die verwendete SINUMERIK 840D verfügte bereits zu diesem Zeitpunkt über integrierte Sicherheitsfunktionen. Der Funktionsumfang umfasste damals (wie heute) die parametrierbare (!) Überwachung von Stillstand, Geschwindigkeit und Positionen bzw. Endlagen. Mit dem aktuellen Sicherheitspaket SINUMERIK Safety Integrated werden an der Prüfanlage zusätzlich neue Funktionen eingesetzt; hier zu nennen sind:

- **Sichere programmierbare Logik (SPL)**

Alle sicherheitsgerichteten Sensoren und Aktoren werden direkt, ohne externe Auswertegeräte, an die E/A-Peripherie der Steuerung angeschlossen und softwaremäßig ausgewertet. Diese sichere, softwaremäßige Verknüpfung führt zu einer hohen Flexibilität bei der Umsetzung einer praxisgerechten Anlagenbedienung. Zusätzlich entsteht ein hoher wirtschaftlicher Nutzen durch die Substitution von konventionellen Hardwarekomponenten.

- **Erweiterte Stopfunktionen**

Mit Einführung der Funktion „externer Stop“ ist es möglich geworden, Teile der Prüfanlage auch bei ausgelösten Sicherheitssignalen unterbrechungsfrei bzw. einfach fortsetzbar zu betreiben. Tritt eine Person (zumeist zufällig und unbeabsichtigt) oder der Prüfer selbst während der Prüfung in das Schutzfeld – als Beispiel eines der Schutzfelder 2 oder 3 (SF2/SF3 in Bild 10/3) – so verringert sich die Geschwindigkeit des Portalläufers (Achsen X/Y) auf eine „sicher reduzierte Geschwindigkeit“, bleibt aber nicht „produktionsstörend“ stehen oder führt gar zu einem Programmabbruch. Ein zeitaufwändiger Programmvorlauf für die Fortsetzung der Prüfung bleibt dem Prüfer dadurch erspart, wobei seine Sicherheit in jeder Situation gegeben bleibt. Denn auch für den Z-Läufer wird je nach dessen momentaner Position intelligent entschieden, ob ein Stop oder die sicher reduzierte Geschwindigkeit aktiviert werden muss.

- **Erweiterte Status- und Diagnoseanzeige**

Zur schnellen und einfachen Diagnose kann nun über eine Softkey-Leiste die gewünschte Information über den Status der Sicherheitsfunktionen in der Anlage direkt angezeigt werden. Darüber hinaus wurden grafische, anwendungsspezifische Diagnose-Statusbilder in die Bedienung integriert.

Bild 10/6
Software ersetzt Hardwarekomponenten, Schaltschränke werden kleiner

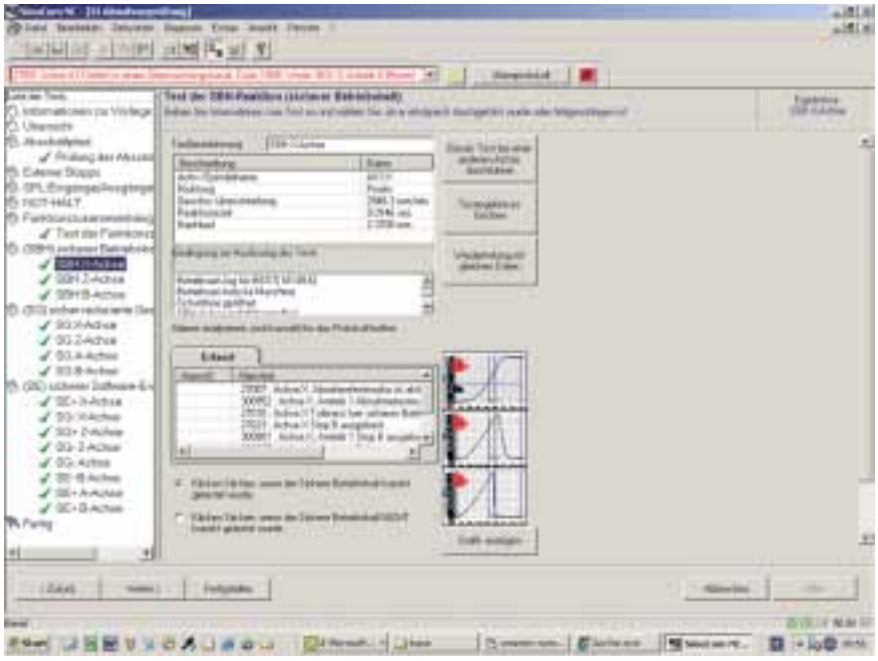


Bild 10/7
Integrierter Abnahmetest mit Bedienerführung und Klartextanzeige als Nachweis für Maschinenhersteller und Endanwender

• **Integrierter Abnahmetest**
Die Sicherheitsfunktionen elektrischer Antriebe sind nach Vorgaben relevanter Normen, bei der Inbetriebnahme durch einen Abnahmetest zu prüfen. Damit der Anwender diesen Test möglichst einfach und schnell durchführen kann, wurde ein „Tool" zur Unterstützung in das Steuerung-/Antriebssystem integriert. Dies verkürzt die Abnahmezeiten erheblich, da z.B. relevante Maschinendaten automatisch übernommen werden. Der geführte Testablauf mit Klartextanzeigen vereinfacht dabei die Bedienung. Selbst das notwendige Abnahmeprotokoll entsteht automatisch.

Betriebserfahrungen: Ein Höchstmaß an Flexibilität, Verfügbarkeit und Sicherheit

Eine (Prüf-)Maschine zu betreiben, die situationsbezogen jeweils ein maßgeschneidertes sicherheitsbezogenes Verhalten zeigt, „gibt ein gutes Gefühl" aus der Sicht eines Prüfers, der durch die neuen Stopfunktionen bei ungewolltem oder beabsichtigten Betreten der Gefahrbereiche in der Prüfung einer Schutzeinrichtung nicht mit lästigen Unterbrechungen, Abbrüchen oder einem erforderlichen Neubeginn der Prüfung konfrontiert ist. Der Wunsch nach einfacher Handhabung und schnellen (Prüf-) Abläufen ging ebenso in Erfüllung. So kann dieser modernen Sicherheitstechnik zugesprochen werden, ein Höchstmaß an Flexibilität und Verfügbarkeit mit dem bestmöglichen Schutz für Personen zu vereinen – „Safety (is) integrated"!

Torsten Borowski
Berufsgenossenschaftliches Institut für Arbeitsschutz (BIA); Sankt Augustin
Fachbereich 5 „Unfallverhütung"
Peter Keil
Siemens AG, Erlangen
A&D MC, Automation and Drive, Motion

10.12 Sicherheit und Taktgefühl

Safety Integrated bei komplexen Sonderwerkzeugmaschinen

Zeit ist Geld. Wer bei der Teileproduktion Geld verdienen, bzw. einsparen will, muss schnell sein. Die ausgeklügelten Maschinenkonzepte der August Wenzler GmbH in Spaichingen ermöglichen Zykluszeiten ihrer Rundtransfermaschinen für Grossbearbeitungen, von denen manche nur träumen. Auch bei der Sicherheitstechnik sind innovative Lösungen gefragt. Bei den drei großen Rundtaktmaschinen, die Opel bei der Firma Wenzler bestellte, feierte „Safety Integrated' einen gelungenen Einstand.

Die Fa. Wenzler erzeugt mit ihrer Technologie hochgenaue und komplexe Werkstücke, wie z.B. Fahrwerkskomponenten. Beim konkret betrachteten Fall wurden Radträger und Schwenklager aus Aluminium, bei einer Stückzeit von nur 17 Sekunden, bearbeitet. Ein Spitzenwert, der ihr neben anderen Qualitäten wie günstigem Preis-Leistungsverhältnis, flexiblen Einrichtungsmöglichkeiten der Maschinen und die Erfahrungen welche Wenzler schon bei anderen Projekten in der Automobilindustrie gemacht hatte, den Auftrag von Opel über drei große Rundtaktmaschinen zur Bearbeitung von Fahrwerkskomponenten einbrachte. Selbst für die High-Tech-Schmiede Wenzler nicht gerade alltäglich: Jede Maschine hat 72 NC-Achsen.

Die Maschine, in ihrer heutigen Ausprägung, wurde in den letzten 20 Jahren in mehreren Stufen entwickelt.

Ab dem Jahr 1983 wurde die Maschine mit einer eigenentwickelten CNC-Steuerung ausgestattet.
Ende der 90er Jahre stieg Wenzler dann auf Siemens-Steuerungen um.

Wenzler hat heute rund 70 Mitarbeiter und baut pro Jahr acht bis zehn Maschinen, die größtenteils an die Automobilindustrie geliefert werden. Der Wert solcher großen Maschinen beträgt leicht 1,5 bis 2,5 Mio. Euro, je nach Ausführung.

Hohe Produktivität auf engstem Raum

Bei der Wenzler MSC-8 B (Multispindelcentrum) handelt es sich um eine 8-Stationen-Maschine. Die 8 Werkstücke können von bis zu 14 Werkzeugen gleichzeitig bearbeitet werden.
Die Werkstücke sind auf schwenkbaren Satellitentische angebracht, so dass eine 5-Seitenbearbeitung oder, durch automatisches Umlegen, auch eine 6-Seitenbearbeitung möglich ist. Durch ihre strikte Modularität erhielt diese flexible Zelle den Charakter einer standardisierten Rundverkettung mit der Leistungsfähigkeit einer Sondermaschine. Jede Bewegung ist CNC-gesteuert, so dass in einem Bearbeitungskubus von 400 x 400 x 400 mm die Maschine bei voller Flexibilität genutzt werden kann.
Das Zentralelement, die 8-eckige Trommel, welche die Werkstücke trägt, ist hängend angeordnet, was einen optimalen Spänefluss und eine gute Zugänglichkeit des Trommellagers und der Spannvorrichtung gewährleistet.
Auf der elektrischen Seite ist die MSC-8B mit der Maschinensteuerung Sinumerik 840D von Siemens ausgerüstet, den dazu passenden Antrieben Simodrive 611D und den Dauermagneterregten Synchronmotoren 1FT6, sowie mit dem Feldbus Profibus. Dazu kommen eine Reihe dezentraler Einheiten. Seit neuestem setzt Wenzler nun auch auf die integrierten Sicherheitsfunktionen „SINUMERIK Safety Integrated".

Integrierte Sicherheitstechnik

Als erster Antriebshersteller weltweit hat Siemens vor gut fünf Jahren integrierte Sicherheitsfunktionen für Personen- und Maschinenschutz auf den Markt gebracht.

Bei der Integration von Sicherheitsfunktionen übernimmt das Antriebssystem und die CNC-Steuerung zusätzlich zu ihren Steuerungs- auch Sicherheitsfunktionen. Dazu gehören die sichere Überwachung von Geschwindigkeit, Stillstand und Position, sowie Funktionen zur sicheren logischen Verknüpfung von Signalen.

Die logische Verknüpfung und die Reaktionen erfolgen intern. Grundsätzlich führen alle sicherheitsrelevanten Fehler im System zu einem sicheren Stillsetzen der Gefahr bringenden Bewegung und zur schnellen kontaktfreien Energietrennung zum Motor. Das Stillsetzen erfolgt stets optimal angepasst an den Maschinenzustand. Das bedeutet hohen Personenschutz im Einrichtbetrieb und zusätzlichen Schutz für Maschine, Werkzeug und Werkstück im Automatikbetrieb.
Safety Integrated ist bereits an über 13.500 Maschinen mit über 80.000 Antrieben im Einsatz. Auf ein entsprechend großes Know-how für Projektierungen neuer Sicherheitskonzepte können Maschinenhersteller zugreifen. Bei den Opel-Maschinen von Wenzler ging es aber um 72 CNC-Achsen und insgesamt 99 Antriebe pro Maschine.

Dies stellte sowohl Wenzler wie auch Siemens vor neue Herausforderungen - insbesondere weil nahezu alle Funktionen von Safety Integrated, einschließlich dem sicheren Bremsenmanagement als Absturzsicherung für Vertikalachsen, verwirklicht werden sollten.

Das Opel Projekt

Die Wenzler Maschinen wurden beim Opel Projekt zur Herstellung der Radträger und Achsschenkel aus Aluminium eingesetzt, wobei jeder Typ in Links/Rechts-Ausführung gleichzeitig gefahren wird. So dass nach 4 Werkstücken die Komponenten für 1 Auto gefertigt sind. Radträger und Achsschenkel aus Aluminium sind relativ neu im Fahrwerksbau. Bisher wurden bei Opel diese Teile aus Guss (GGG) hergestellt. Das Streben nach Gewichtsreduzierung, speziell der ungefederten Massen im Fahrwerksbau, führen zur Verbesserung der Agilität und des Fahrkomforts. So konnte durch die neue Aluminium-Ausführung eine Reduzierung des Gewichts um 6,6 kg erzielt werden.

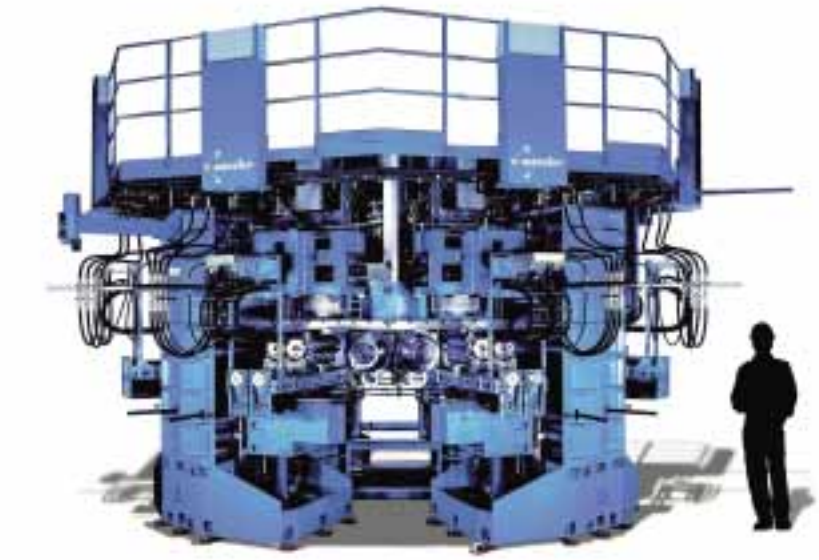
„Das Projekt startete im Spätherbst 2000. In Zusammenarbeit wurde zunächst ein Grobkonzept entworfen, welches aufzeigte, wie so umfangreiche Safety Integrated-Applikationen überhaupt angegangen werden können“, so Ingrid Hölzer, auf Siemens-Seite mit dieser Aufgabe betraut. Dieses Konzept baut auf der von der Firma Wenzler definierten Steuerungsstruktur auf, die aus acht NCUs besteht. Für die Safety Integrated Funktionalität wurde NCU1 als Master definiert. Danach schrieben die Spezialisten von Wenzler, namentlich Ralf Rottler, die nötigen Software-Teile für die NC- und die SPS-Seite der Steuerung. Dieses ist laut Ingrid Hölzer „erstaunlich gut gelungen. Die Kommunikation bis auf die Ebene der Einrichter ist vorbildlich gelaufen".

Höherer Schutz und Flexibilität

Die Vorteile, die Wenzler nun sieht, liegen laut Jürgen Ruffieux, Leiter der Elektronik-Entwicklung , „primär in einem höheren Schutz während des Einrichtebetriebs, sowie in der höheren Flexibilität für das Einrichtepersonal."

Das früher übliche Überbrücken von Sicherheitseinrichtungen während des Einrichtbetriebs entfällt. Die Einrichter sind stets geschützt.

Opel erhofft sich von Safety Integrated weniger Aufwand beim Aufbau der Maschine, kürzere Reaktionszeiten und mehr Sicherheit durch die automatische Selbstdiagnose und die kreuzweise Überwachung durch SPS und NC. Die Serienproduktion mit den neuen Maschinen begann im ersten Quartal 2002.



Die Wenzler MSC- 8B, eine modular aufgebaute Rundtaktmaschine, die bei Opel mit 72 NC- Achsen ausgestattet ist. Die "nackte" Maschine zeigt den Aufbau aus einzelnen ähnlichen Grundelementen

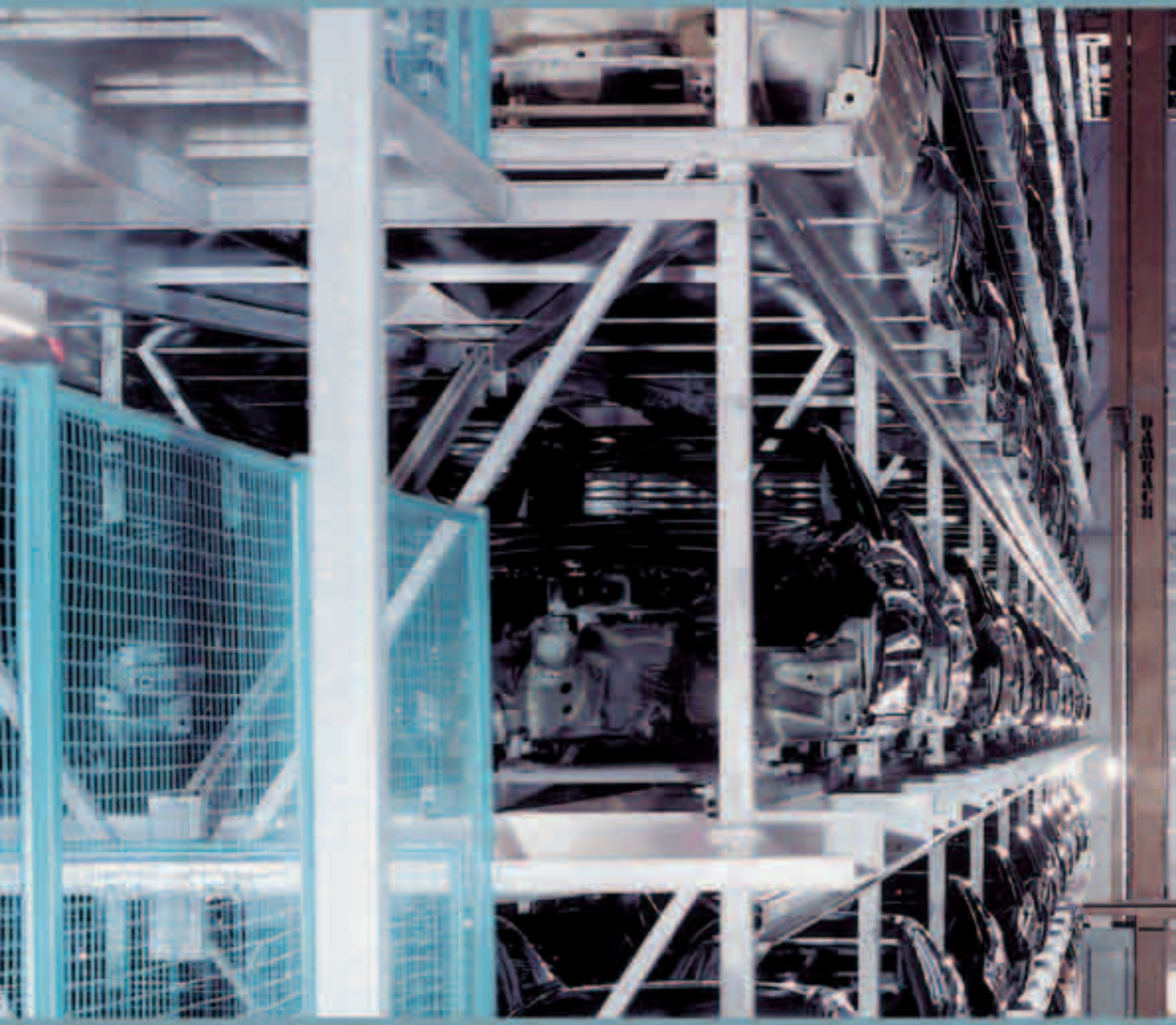
Aluminium spart Gewicht im Auto. Im konkreten Fall bei Opel, spart der Werkstoff bei Radträgern und Achsschenkeln 6,6 kg gegenüber früheren Graugussteilen ein

10.13 Sicherer Halt in der Druckindustrie

Zunehmende Produktivitätssteigerung und hohes Kostenbewußtsein im Bereich der Druckmaschinenindustrie führen dazu, daß klassische, mechanische Lösungen (wie z.B. die Königswelle) durch elektrische Antriebstechnik ersetzt werden (Mechatronic). Dies stellt aber andererseits immer höhere Anforderungen an die zur Überwachung der Antriebe notwendige Sicherheitstechnik. Wo vorher nur einige wenige Antriebe sicherheitstechnisch überwacht werden mußten, muß bei den heutigen, neuen Konzepten eine Vielzahl von Antrieben in die Betrachtung mit einbezogen werden.

Ein besonderes Gefährdungspotenzial für das Bedienpersonal besteht vor allem bei Arbeiten in der Anlage mit geöffneten Schutzvorrichtungen. Hier wird vom Gesetzgeber gefordert, daß Personen durch geeignete Einrichtungen vor einem ungewollten Anlauf der Antriebe geschützt werden müssen.

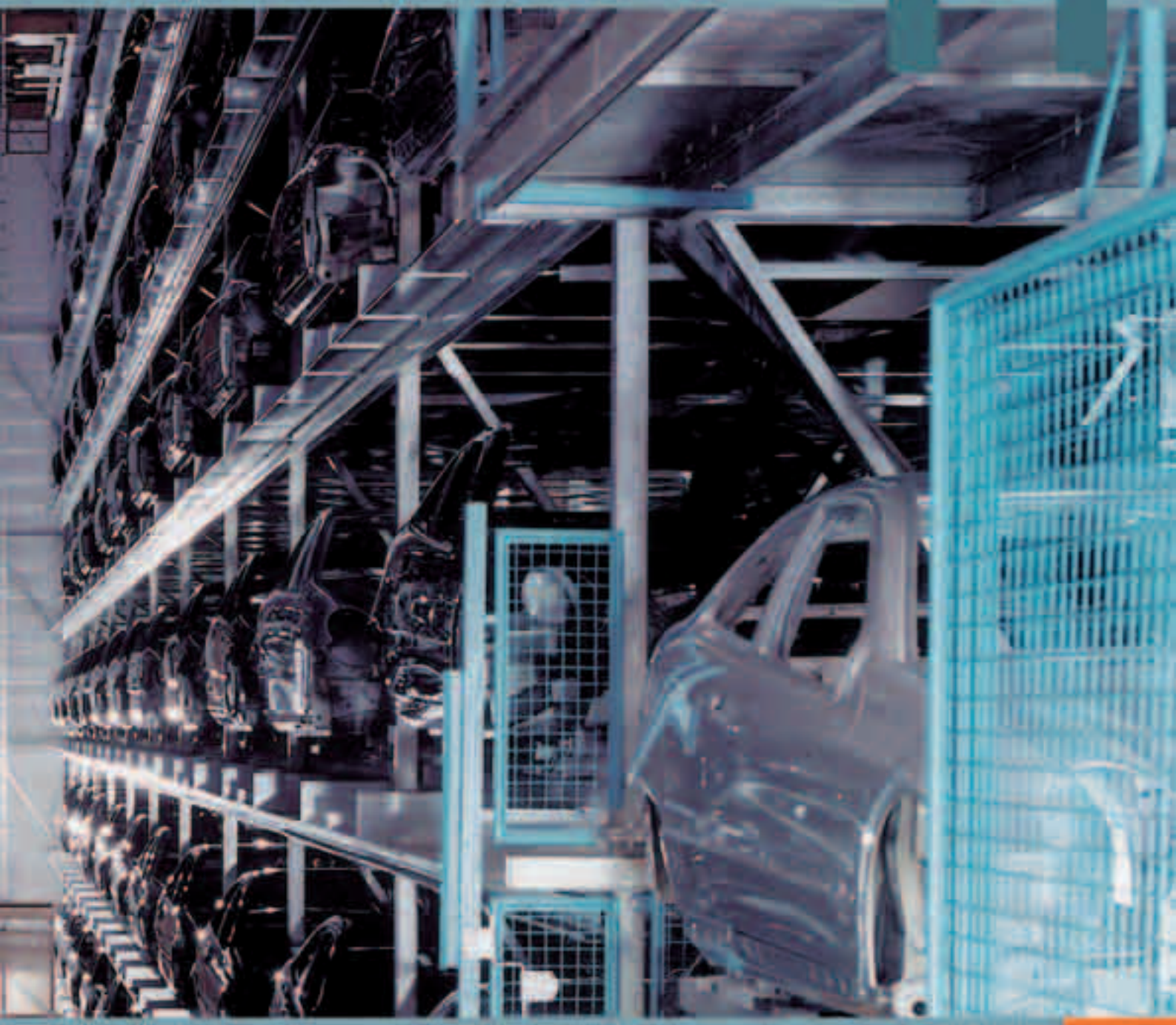
Durch Einsatz der Gerätereihe SIMOVERT MASTERDRIVES, welche mit einem integrierten Sicherheitsrelais diese Schutzfunktion gegen ungewollten Anlauf des Antriebs unterstützt, konnte das vorher notwendige, motorseitige Schütz eingespart werden. Da in der Druckmaschinenindustrie Anlagen mit weit über hundert Antrieben keine Seltenheit sind, führte diese Einsparung durch Wegfall der Material- und Montagekosten sowie eine geringere Montagefläche im Schaltschrank zu einer erheblichen Kosten- und Zeitreduzierung.



11.1 Begriffe und Abkürzungen
11.2 Literatur
11.3 Kontakt - Internet und Hotlines
11.4 Seminarangebot - Sicherheitstechnik, Normen und Richtlinien
11.5 Stichwortverzeichnis

11

Anhang



11 Anhang

11.1 Begriffe und Abkürzungen

Begriffe

Anforderungsklasse (AK)

Maß für die sicherheitsbezogene Leistungsfähigkeit von Steuerungseinrichtungen. Definiert in DIN V 19250 und DIN V VDE 0801.

Aktor

Wandler, der elektrische Signale in mechanische oder andere, nichtelektrische Größen umsetzt.

Ausfall / Fehler

Ausfall

Beendigung der Fähigkeit eines Betriebsmittels zur Ausführung einer geforderten Funktion.

Fehler

Ungewollter Zustand eines Betriebsmittels, gekennzeichnet durch die Unfähigkeit, eine geforderte Funktion auszuführen.

Hinweis: Der „Ausfall" ist ein Ereignis und der „Fehler" ein Zustand.

Blanking

Durch Blanking wird ein bestimmter Ausschnitt aus dem Schutzfeld z.B. eines Lichtvorhanges oder Lichtgitters ausgeblendet, d.h. unwirksam gemacht. Es gibt zwei Arten: Fixed (feststehendes) und Floating (bewegliches) Blanking.

Fixed Blanking

Beim Fixed Blanking ist der ausgeblendete Bereich fest. Diese Funktion wird z.B. angewendet, wenn fest stehende Einrichtungen in das Schutzfeld ragen.

Floating Blanking

Floating Blanking erlaubt, dass normalerweise ein oder zwei Lichtstrahlen im Schutzfeld unterbrochen sind, ohne dass ein Stop-Signal vom Lichtvorhang ausgegeben wird. Diese Funktion wird benötigt, wenn sich die „erlaubte" Unterbrechung der Lichtstrahlen nicht auf eine feste Position im Schutzfeld bezieht, z.B. wenn ein bewegliches Kabel das Schutzfeld durchdringt.

Fehler

Siehe „Ausfall / Fehler".

Fehlersicher

Fähigkeit einer Steuerung, auch beim Auftreten von Fehlern (Ausfällen) einen sicheren Zustand der gesteuerten Einrichtung (z.B. Maschine, Prozess) zu erhalten oder die Einrichtung in einen sicheren Zustand zu bringen.

Fehlertoleranz

Fehlertoleranz N bedeutet, dass eine Einrichtung bei Vorhandensein von N Fehlern die vorgesehene Aufgabe noch ausführen kann. Bei N+1 Fehlern versagt die Einrichtung bei der Ausführung der vorgesehenen Funktion.

Gefährdung

Potenzielle Quelle eines Schadens. (aus EN 292-1 bzw. ISO 12100-1)

Z.B. Gefährdung durch elektrischen Schlag, Gefährdung durch Quetschen, ...

Kanal

Element oder Gruppe von Elementen, das/die eine Funktion unabhängig ausführt.

2-kanalige Struktur

Struktur, die eingesetzt wird, um Fehlertoleranz zu erreichen.

Z.B. eine 2-kanalige Schützansteuerung ist dann erreichbar, wenn mindestens zwei Freigabekreise zur Verfügung stehen und der Hauptstrom redundant abgeschaltet wird oder ein Sensor (z.B. Not-Halt-Schalter) wird mit zwei Kontakten abgefragt und jeweils getrennt zum Auswertegerät geführt.

Kategorie

In EN 954-1 (prEN ISO 13849-1) verwendet zur „Einteilung der sicherheitsbezogenen Teile einer Steuerung in Bezug auf ihre Widerstandsfähigkeit gegen Fehler und ihr Verhalten im Fehlerfall, die aufgrund der strukturellen Anordnung der Teile und/oder deren Zuverlässigkeit erreicht wird."

Lastgruppe

Eine Gruppe von Motorstartern, die von einer Energiebus-Einspeisung versorgt werden. Eine Lastgruppe kann sich innerhalb einer Potenzialgruppe befinden oder Teile von zwei Potenzialgruppen umfassen.

Motorstarter (MS)

Motorstarter ist der Oberbegriff für Direkt- und Reversierstarter. Mit dem Motorstarter werden Anlauf und Drehrichtung bestimmt.

Direktstarter

Ein Direktstarter ist ein Motorstarter für eine Drehrichtung, der einen Motor direkt ein- oder ausschaltet. Er besteht aus einem Leistungsschalter und einem Schütz.

Reversierstarter

Ein Reversierstarter ist ein Motorstarter für zwei Drehrichtungen. Er besteht aus einem Leistungsschalter und zwei Schützen.

Muting

Zeitbegrenztes bestimmungsgemäßes Aufheben von (einer) Sicherheitsfunktion(en).

Not-Aus

Not-Aus-Einrichtung

Anordnung von Bauteilen, die dazu bestimmt ist, die Not-Aus-Funktion zu verwirklichen (EN 418 bzw. ISO 13850). (Hinweis: heute unterscheidet man „Stillsetzen im Notfall" und „Ausschalten im Notfall")

Stillsetzen im Notfall

Funktion, die aufkommende oder bestehende Gefährdungen für Personen, Schäden an der Maschine oder bei der Durchführung von laufenden Arbeiten abwenden oder mindern soll;

– durch eine einzige Handlung einer Person ausgelöst wird. (EN 291-1 bzw. ISO 12100-1)

Ausschalten im Notfall

Ein Ausschalten im Notfall wird durch Abschalten der Maschine von der Versorgung erreicht, mit der Folge eines Stops der Kategorie 0 (EN 60204 1997). Ein Ausschalten im Notfall sollte gemäß EN 60204-1 1997 dort vorgesehen werden, wo die Möglichkeit einer Gefährdung durch Elektrizität besteht.

Not-Halt

Eine Handlung im Notfall, die dazu bestimmt ist, einen Prozess oder eine Bewegung anzuhalten, der (die) gefahrbringend wurde (aus EN 60204-1 Anhang D).

Potenzialgruppe

Eine Gruppe von Motorstartern und/oder Elektromodulen, die von einem Powermodul versorgt werden.

Redundanz

Vorhandensein von mehr als für die Ausführung der vorgesehenen Aufgaben an sich notwendigen Mittel.

Risiko

Kombination der Wahrscheinlichkeit eines Schadeneintritts und des Schadenausmaßes.

Rückführkreis

Stromkreis zur Überwachung der angesteuerten Schütze.

Die Funktion der Schütze kann überwacht werden, indem die zwangsgeführten Hilfskontakte von einem Auswertegerät rückgelesen werden. Ist ein Schütz verschweißt, verhindert das Auswertegerät einen Wiederstart.

Safety Integrity Level (SIL)

In IEC 61508 definiertes Maß für die sicherheitsbezogene Leistungsfähigkeit (Safety performance) einer elektrischen oder elektronischen Steuerungseinrichtung. (-> Kapitel 1)

Sicherheit

Freiheit von unakzeptablem Risiko.

Funktionale Sicherheit

Der Teil der Sicherheit einer Einrichtung (z.B. Maschine, Anlage), der von der korrekten Funktion abhängt.

Sicherheitsfunktion

Funktion (z.B. einer Maschine oder einer Steuerung), deren Ausfall (oder Versagen) das Risiko/die Risiken erhöhen kann.

Sicherheitsfunktionen von Steuerungen (EN 954 bzw. prEN ISO 13849-1)

„Durch ein Eingangssignal ausgelöste und durch sicherheitsbezogene Teile von Steuerungen verarbeitete Funktion, die der Maschine (als System) das Erreichen eines sicheren Zustandes ermöglicht."

Sicherheitsrelevante Steuerungsfunktion (IEC 62061)

Steuerungsfunktion, die durch ein sicherheitsrelevantes Steuerungssystem ausgeführt wird, um einen sicheren Zustand einer Einrichtung (z.B. Maschine) zu erhalten oder das Entstehen gefährlicher Zustände zu vermeiden.

Sicherheitsrelevante Steuerungsfunktion

Hier gibt es in verschiedenen Normen geringfügig unterschiedliche Definitionen.

Sicherheitsziel

Gefährdung von Mensch und Umwelt so gering wie möglich halten, ohne dadurch die industrielle Produktion, den Einsatz von Maschinen oder die Herstellung von chemischen Produkten mehr als unbedingt erforderlich einzuschränken.

Stillsetzen

Funktion, die aufkommende oder bestehende Gefährdungen für Personen, Schäden an der Maschine oder bei der Durchführung von laufenden Arbeiten abwenden oder mindern soll. Vorrang vor allen Betriebsarten.

Stop-Kategorie

In EN 60204-1 verwendeter Begriff zur Bezeichnung von drei verschiedenen Stillsetzfunktionen.

Teilpotenzialgruppe

Eine Teilpotenzialgruppe besteht dann, wenn innerhalb einer Potenzialgruppe die Hilfsspannung teilweise abgeschaltet werden kann.

Zustimmeinrichtung

Zusätzliche handbetätigte Steuereinrichtung, die eine bestimmte Funktion einer Maschine zulässt, wenn sie ständig betätigt wird.

Zweihandschaltung

Steuereinrichtung, die mindestens die gleichzeitige Betätigung durch beide Hände erfordert, um gefährdende Maschinenfunktionen in Gang zu setzen und aufrecht zu erhalten.

Abkürzungen

ANSI	American National Standards Institute
BIA	Berufsgenossenschaftliches Institut für Arbeitssicherheit
BWS	Berührungslos wirkende Schutzeinrichtungen
CNC	Computerised Numerical Control
CPU	Central Processing Unit
DMS	Direktes Messsystem
FTS	Fahrerloses Transportsystem
HMI	Human Machine Interface
IBS	Inbetriebsetzung
IMS	Indirektes Messsystem
KDV	Kreuzweiser Datenvergleich
MLFB	Maschinenlesbare Fabrikatenummer: Bestellnummer von Siemens-Komponenten
NC	Numerical Control
NCK	Numerical Control Kernel
NCU	Numerical Control Unit
NFPA	National Fire Protection Association
OP	Operator Panel
OSHA	Occupational Safety and Health Administration
PLC	Programmable Logic Control
PM	Positiv-Masseschaltend
PP	Positiv-Positivschaltend
S5	SIMATIC S5
S7	SIMATIC S7

11.2 Literatur

[1] Positionspapier DKE 226.0.3: Sicherheitsgerichtete Funktionen elektrischer Antriebssysteme in Maschinen. Stand 1/98.

[2] Schaefer, M.; Umbreit, M.: Antriebssysteme und CNC-Steuerungen mit integrierter Sicherheit. BIA-Report Nr. 4/97

[3] Kategorien für sicherheitsbezogene Steuerungen nach EN 954-1. BIA-Report 6/97.

[4] ZH1/419. Prüf- und Zertifizierungsordnung der Prüf- und Zertifizierungsstellen im BG-Prüfzert. Ausgabe 10/1997.

[5] Reinert, D.;Schaefer, M.; Umbreit, M.: Antriebe und CNC-Steuerungen mit integrierter Sicherheit. In: ETZ-Heft 11/98

[6] Sicherheitsrelevante Datenübertragung; Anforderungen sowie deterministische und probabilistische Verfahren; 1998, Uwe Jesgarzewski, Rainer Faller – TÜV Product Service

11.3 Kontakt – Internet Hotlines

Internetadresse:

Allgemein

http://www.siemens.de/safety
http://www.siemens.de/automation

AS-Interface

http://www.siemens.de/as-interface

SIRIUS

http://www.siemens.de/sirius

SIGUARD

http://www.siemens.de/siguard

SIMATIC

http://www.siemens.de/simatic-controller
http://www.siemens.de/simatic-dp

SIMODRIVE 611, SIMODRIVE POSMO, SIMOVERT MASTERDRIVES

http://www.siemens.de/simodrive

SINUMERIK

http://www.siemens.de/sinumerik

Hotlines:

SIMATIC
++49(0)911-895-7000

SIRIUS
++49(0)911-895-5900

SINUMERIK
++49(0)180-5258008

11.4 Seminarangebot – Sicherheitstechnik, Normen und Richtlinien

Denn das Training entscheidet über Ihren Erfolg

SITRAIN® - das Siemens Training for Automation and Industrial Solutions - steht Ihnen bei der Bewältigung Ihrer Aufgaben umfassend zur Seite.

Mit Training vom Marktführer in der Automatisierung, Anlagenerrichtung und -betreuung gewinnen Sie an Sicherheit und Souveränität in Ihren Entscheidungen. Gerade wenn es um den optimalen Einsatz von Produkten und die effiziente Nutzung von Anlagen geht. Sie können Defizite bestehender Anlagen beseitigen und teure Fehlplanungen von vornherein ausschließen.

Unterm Strich bedeutet das einen enormen Gewinn für Ihren Betrieb: verkürzte Anlaufzeiten, optimierte Anlagenteile, schnellere Fehlerbehebung, verringerte Ausfallzeiten. Also mehr Ertrag und weniger Kosten.

Top-Trainer

Unsere Trainer kommen direkt aus der Praxis und verfügen über umfangreiche didaktische Erfahrungen. Die Kursentwickler haben einen direkten Draht zur Produktentwicklung und geben ihr Wissen direkt an die Trainer weiter.

Praxisnähe

Diese Praxisnähe der Trainer macht es möglich, Ihnen das theoretische Wissen wirklich plausibel zu machen. Aber da alle Theorie bekanntlich grau ist, legen wir höchsten Wert auf praktische Übungen, die bis zur Hälfte der Kurszeit einnehmen. Im Arbeitsalltag können Sie das Gelernte also sofort umsetzen. Wir schulen Sie an modernsten, methodisch-didaktisch konzipierten Trainingsgeräten. So trainiert fühlen Sie sich absolut sicher.

Lernvielfalt

Mit insgesamt etwa 300 Präsenzkursen schulen wir das gesamte Spektrum der A&D-Produktwelt und einen Großteil der Anlagenlösungen von I&S. Fernlehrgänge, Selbstlernsoftware und moderierte Seminare im Web ergänzen unser klassisches Kursangebot.

Kundennähe

Der Weg ist nicht weit. Sie finden uns ca. 60 mal in Deutschland und weltweit in 62 Ländern. Sie möchten statt einem unserer 300 Kurse ein ganz individuelles Training? Unsere Lösung:
Wir schneidern Ihnen das Programm persönlich auf Ihren Bedarf zu.

Trainiert wird in unseren Trainings-Centern oder bei Ihnen im Betrieb.

Die richtige Mischung: Blended Learning

Unter Blended Learning versteht man die Kombination von verschiedenen Lernmedien und -sequenzen. So kann beispielsweise ein Präsenzkurs in einem Trainings-Center durch Selbstlernprogramme zur Vor- oder Nachbereitung optimal ergänzt werden. Ergänzend nutzt SITRAIN moderiertes Online-Lernen, um zu vereinbarten Zeitpunkten live im Internet Unterricht zu halten.

Die Mischung macht's. Deswegen kann Blended Learning so gut komplexe Themen vermitteln und das vernetzte Denken schulen. Zusatzeffekt: weniger Reisekosten und Ausfallzeiten durch orts- und zeitunabhängige Trainingssequenzen.

Das internationale Lernportal

www.siemens.de/sitrain

Alle Lernmöglichkeiten auf einen Blick! Recherchieren Sie bequem im weltweiten Lernangebot, rufen Sie online alle Kurstermine ab, nutzen Sie die tagesaktuelle Anzeige von freien Kursplätzen - und melden Sie sich direkt an.

Themen	Zielgruppe	Dauer	Kurztitel
Safety Integrated Überblick für Planer	Entscheider, Vertriebspersonal, Projektleiter, Projektmitarbeiter	2 Tage	ST-SIUEBP
Safety Integrated für Entwickler	Programmierer	3 Tage	ST-SIUEBE
Safety Integrated Überblick in der Fertigungsindustrie	Entscheider, Vertriebspersonal, Projektleiter, Projektmitarbeiter, Programmierer, Inbetriebsetzer, Projektierer	2 Tage	ST-SIUEBF
Projektieren und Programmieren mit Distributed Safety	Programmierer, Inbetriebsetzer, Projektierer	3 Tage	ST-PPDS
Projektieren und Programmieren mit F-Systems in STEP7/ PCS7 Umgebung	Programmierer, Inbetriebsetzer, Projektierer	3 Tage	ST-PPFS
SIMATIC S7, S7-400 H Systemkurs	Programmierer, Inbetriebsetzer, Projektierer	3 Tage	ST-7H400H
Produkt- und Anwendungsschulung für berührungslos wirkende Schutzeinrichtungen - SIGUARD	Entscheider, Vertriebspersonal, Inbetriebsetzer, Projektierer, Servicepersonal, Bediener, Anwender	2 Tage	MP-BWS
SINUMERIK 840D, Safety Integrated Wartungskurs	Servicepersonal, Instandhalter	3 Tage	NC-84DSIS
SINUMERIK 840D, Safety Integrated Projektierung und Inbetriebnahme	Inbetriebsetzer, Projektierer, Servicepersonal	5 Tage	NC-84DSIW
Elektromagnetische Verträglichkeit für die Praxis	Programmierer, Inbetriebsetzer, Projektierer, Servicepersonal, Instandhalter	3 Tage	MP-EMVPRA
Explosionsschutz Grundlagen	Entscheider, Vertriebspersonal, Inbetriebsetzer, Projektierer, Servicepersonal, Instandhalter	1 Tag	MP-EX-GRU
Explosionsschutz Eigensicherheit	Entscheider, Vertriebspersonal, Inbetriebsetzer, Projektierer, Servicepersonal, Instandhalter	1 Tag	MP-EX-EIG

Safety Integrated Überblick für Planer (ST-SIUEBP)

In diesem Übersichtskurs lernen Sie alles was für die Planung einer sicheren Anlage benötigt wird. Sie lernen die Gesetze und Normen kennen und wissen, wie die daraus resultierenden Inhalte auf Ihre Anlagenplanung zu übertragen sind.

Inhalte

- Überblick Gesetze / Normen
- Risiko Analyse, SIL Einstufungen, Performance Levels, Safety Category
- Funktionale Sicherheit MM
- Applikationssoftware Entwicklung, V-Modell
- Aufgaben eines Funktionalen Sicherheitsverantwortlichen
- Dokumente die einzufordern bzw. zu liefern sind, Änderungswesen
- Fehlerbetrachtung
- Ausfallwahrscheinlichkeit
- Qualifizierung für das Gesamtsystem - Applikationsbeispiele mit Übung
- Common Cause Fehler
- State of the Art von Sicherheitssystemen
- Siemens Lösungen zur Maschinen- und Prozessleittechnik

Zielgruppe

Entscheider, Vertriebspersonal, Projektleiter, Projektmitarbeiter

Dauer

2 Tage

Teilnahmegebühr

auf Anfrage

Kursort

Mannheim

Safety Integrated Überblick für Entwickler (ST-SIUEBE)

Hier werden Ihnen zusätzlich zu den Inhalten des Übersichtskurses (ST-SIUEBP) die weiteren Informationen für die Berechnungen einer sicheren Anlage erläutert. In praxisnahen Beispielen und Übungen wird das erlangte Wissen vertieft.

Inhalte

- Überblick Gesetze / Normen
- Risiko Analyse, SIL Einstufungen, Performance Levels, Safety Category
- Funktionale Sicherheit MM
- Applikationssoftware Entwicklung, V-Modell
- Aufgaben eines Funktionalen Sicherheitsverantwortlichen
- Dokumente die einzufordern bzw. zu liefern sind, Änderungswesen
- Fehlerbetrachtung
- Ausfallwahrscheinlichkeit
- Qualifizierung für das Gesamtsystem
- Applikationsbeispiele mit Übung
- Common Cause Fehler
- State of the Art von Sicherheitssystemen
- Siemens Lösungen zur Maschinen- und Prozessleittechnik
- FMEDA (Failure Modes, Effects and Diagnostic Analysis)
- ULM für Sicherheitstechnik
- Qualifizierung Common Cause
- Markov Modelle
- Grundsätzliche Systemstrukturen
- Beispiele und Übungen

Zielgruppe

Programmierer

Dauer

3 Tage

Teilnahmegebühr

Auf Anfrage

Kursort

Mannheim

Safety Integrated Überblick in der Fertigungstechnik (ST-SIUEBF)

Dieser Kurs zeigt Ihnen zum einen die aktuelle Normenlage in der Fertigungstechnik auf, zum anderen lernen Sie anhand ausgewählter Beispiele die fachgerechte Anwendung in der Praxis. Ziel des Kurses ist es, Theorie und Praxis zusammen zu führen. Durch die kompetente Realisierung im eigenen Betrieb sichern Sie das Produktionsergebnis und erzielen Vorteile im Wettbewerb.

Inhalte

- EG-Maschinenrichtlinie
  - Grundlagen, Definitionen, Anforderungen, Umsetzung, Anwendung auf neue Maschinen und neue Maschinenanlagen
  - Anwendung bei Veränderungen und Modernisierung
  - Konformitätsbewertung
- EG-Niederspannungsrichtlinie
  - Grundlagen, Definitionen, Anforderungen, Umsetzung
- Überblick Normen
  - EN ISO 12 100 (EN 292), EN 1050 (ISO 14121)
  - EN 60204-1
  - EN 954-1, (prEN ISO 13849-1), EN ISO 13849-2, (EN 954-2)
  - EN 62061, IEC 61508
- Praxisbeispiel Automobilindustrie, (Lackiererei Nachbehandlung mit Transport über ein Schienensystem)
  - Normen und Anwendung
  - Verwendung und Einsatz
  - Aufbau, Realisierung und Umsetzung der Risiko-Analyse anhand konventioneller Verdrahtung bzw. busbasierten Lösungen.

Zielgruppe

Entscheider, Vertriebspersonal, Projektleiter, Projektmitarbeiter, Programmierer, Inbetriebsetzer, Anwender

Dauer

2 Tage

Teilnahmegebühr

Auf Anfrage

Kursort

Nürnberg, Mannheim

Projektieren und Programmieren mit Distributed Safety (ST-PPDS)

Die Teilnehmer lernen die Handhabung, Projektierung, Programmierung, Inbetriebnahme, Diagnose und Fehlerbehebung der Distributed Safety Systeme. Diese umfassen die fehlersicheren Zentralbaugruppen CPU 315F-2DP, CPU 317F-2DP, CPU 416F DP und der IM151-F CPU. Die fehlersichere Programmierung erfolgt in den Programmiersprachen F-FUP bzw. F-KOP.

Inhalte

Überblick Normen und Richtlinien

- AS S7-300F (Prinzip, Systemaufbau und Peripherie)
- Projektierung der fehlersicheren Peripherie mit Distributed Safety
- Programmierung eines sicherheitsgerichteten Anwenderprogramms
- Fehlersichere Kommunikation PROFIsafe (CPU-CPU-Kommunikation, Master Slave Kommunikation)
- Diagnosemöglichkeiten (CPU-Diagnose, Peripherie-Diagnose, weiterführende Diagnosetools)
- Übungen zum Peripherieaufbau, Kommunikation, Fehlersuche
- Beispiele zur Programmierung (Emergency Stop, Schutztür, sicherheitsgerichtete Abschaltung, Passivierung, Programmierbesonderheiten)

Zielgruppe

Programmierer, Inbetriebsetzer, Projektierer

Dauer

3 Tage

Teilnahmegebühr

Auf Anfrage

Kursort

Essen, Hannover, Mannheim, Nürnberg

Projektieren und Programmieren mit F-Systems in STEP7 / PCS7 Umgebung (ST-PPFS)

Die Teilnehmer lernen die Handhabung, Projektierung, Programmierung, Inbetriebnahme, Diagnose und Fehlerbehebung der FSystems Systeme. Diese umfassen die fehlersicheren - und optional hochverfügbaren - Zentralbaugruppen CPU 414-4 H und CPU 417-4 H. Die fehlersichere Programmierung, durch die diese Zentralbaugruppen sicherheitsgerichtete Applikationen steuern, erfolgt in der Programmiersprache CFC.

Inhalte

- Überblick Redundanztechnik (H-/F-Unterschied, Verfügbarkeit, redundante Systeme, Vorschriften)
- AS S7-400F (Prinzip, Systemaufbau und Peripherie)
- Projektierung der fehlersicheren Peripherie mit F-Systems
- Programmierung eines sicherheitsgerichteten Anwenderprogramms mit CFC
- Fehlersichere Kommunikation Profisafe
- Übungen zum Peripherieaufbau, Kommunikation, Fehlersuche
- Beispiel zur Programmierung, Programmierbesonderheiten

Zielgruppe

Programmierer, Inbetriebsetzer, Projektierer

Dauer

3 Tage

Teilnahmegebühr

Auf Anfrage

Kursort

Essen, Mannheim, Nürnberg

SIMATIC S7, S7-400 H Systemkurs (ST-7H400H)

Die Teilnehmer lernen die Handhabung, Projektierung, Inbetriebnahme, Diagnose und Fehlerbehebung des hochverfügbaren Automatisierungssystems SIMATIC S7-400H.

Inhalte

- Überblick Redundanztechnik (H-/F-Unterschied, Verfügbarkeit, redundante Systeme)
- AS S7-400H (Prinzip, Systemaufbau und Peripherie, Synchronisation, Ankoppeln und Aufdaten der Reserve, Selbsttest, prinzipielle Arbeitsweise, Fehlerverarbeitung)
- Projektierung mit STEP7/HSys (Systemparametrierung, Systemhantierung, Fehlerdiagnose, Dokumentation)
- Übungen zum Peripherieaufbau, zur Fehlersuche, Beispiele zur Programmierung

Zielgruppe

Programmierer, Inbetriebsetzer, Projektierer

Dauer

3 Tage

Teilnahmegebühr

Auf Anfrage

Kursort

Essen, Nürnberg

Produkt- und Anwendungsschulung für berührungslos wirkende Schutzeinrichtungen - SIGUARD (MP-BWS)

Sie lernen in diesem Workshop den Umgang und Einsatz von berührungslos wirkenden Schutzeinrichtungen (Lichtvorhänge, Lichtgitter, und Laserscanner) der SIGUARD-Reihe kennen.

Inhalte

- Europäische Richtlinien
- Sicherheitsbezogene Teile von Steuerungen nach EN 945-1
- Sicherheits-Lichtvorhang SIGUARD
- Sicherheits-Laserscanner SIGUARD
- Berechnungen von Sicherheitsabständen nach EN 999
- Auswertegeräte
- Prüfung von BWS
- Diagnose

Zielgruppe

Entscheider, Vertriebspersonal, Inbetriebsetzer, Projektierer, Servicepersonal, Bediener, Anwender

Dauer

2 Tage

Teilnahmegebühr

Auf Anfrage

Kursort

Mannheim, Nürnberg-Moorenbrunn

SINUMERIK 841D, Safety Integrated Wartungskurs (NC-84DSIS)

Dieser Kurs vermittelt Kenntnisse, die für die Instandhaltung und Wartung einer Maschine mit SINUMERIK 840D und Safety Integrated erforderlich sind. Nach dem Kurs kann der Teilnehmer Fehler finden und beheben, sowie nach Reparatur/Softwarehochrüstung die sicherheitsrelevanten Funktionen überprüfen und abnehmen.

Inhalte

- Allgemeines zur Sicherheitstechnik
- Systemvoraussetzungen
- Beschreibung der sicheren Grundfunktionen
- Sichere programmierbare Logik
- Sensor-/Aktor-Einbindung
- Teststop
- Beschreibung der Maschinendaten und Nahtstellensignale
- Vorgehensweise bei Inbetriebnahme und Fehlersuche
- Auswertung von Diagnose- und Alarmanzeigen
- Schaltungsbeispiele für Safety Integrated
- Abnahmeprotokoll
- Praktische Übungen zu Fehlersuche und Service an Trainingsmodellen mit digitalen Vorschub- und Hauptspindelantrieben

Zielgruppe

Servicepersonal, Instandhalter

Dauer

3 Tage

Teilnahmegebühr

Auf Anfrage

Kursort

Chemnitz, Düsseldorf, Nürnberg-Moorenbrunn

SINUMERIK 840D, Safety Integrated Projektierung und Inbetriebnahme (NC-840DSIW)

Dieser Kurs vermittelt die Projektierung und Inbetriebnahme der Funktion Safety Integrated mit einer SINUMERIK 840D. Nach dem Kurs kann der Teilnehmer mit der Funktion Safety Integrated und einer SINUMERIK 840D spezielle Anlagenkonfigurationen mit Sicherheitsfunktionen projektieren, testen und in Betrieb nehmen.

Inhalte

- Allgemeines zur Sicherheitstechnik
- Systemvoraussetzungen
- Beschreibung der sicheren Grundfunktionen
- Sichere programmierbare Logik
- Sensor-/Aktor-Einbindung
- Teststop
- Sichere Kommunikation mit PROFIsafe
- Sicheres Bremsenmanagement
- Beschreibung der Maschinendaten und Nahtstellensignale
- Vorgehensweise bei Inbetriebnahme und Fehlersuche
- Auswertung von Diagnose- und Alarmanzeigen
- Schaltungsbeispiele für Safety Integrated
- Abnahmeprotokoll
- Praktische Übungen zu Projektierung, Inbetriebnahme und Service an Trainingsmodellen mit digitalen Vorschub- und Hauptspindelantrieben

Zielgruppe

Inbetriebsetzer, Projektierer, Servicepersonal

Dauer

5 Tage

Teilnahmegebühr

Auf Anfrage

Kursort

Nürnberg-Moorenbrunn

Elektromagnetische Verträglichkeit in der Praxis (MP-EMVPRA)

Der Kurs wendet sich an alle Mitarbeiter in Entwicklung, Konstruktion, Fertigung und Service, die praktische Kenntnisse und Fertigkeiten zur EMV für ihre tägliche Arbeit benötigen. Die einzelnen Themen werden durch Videofilme verdeutlicht, praxisbezogene Auswirkungen von EMV-Phänomenen mit entsprechenden Maßnahmen zur Vorbeugung bzw. Abhilfe werden demonstriert. Ziel dieses Trainings ist es, EMV-Störungen verhindern bzw. beheben zu können.

Inhalte

- was Sie bei der Anlagenplanung besonders beachten müssen
- wie ein EMV-gerechter Schaltschrank aussieht, insbesondere mit geregelten Antrieben, Hintergründe der einzelnen Schrankaufbauregeln
- wie zwischen Software-, Hardware- und EMV-Störungen unterschieden werden kann
- welche Messmittel zur Fehlersuche sinnvoll sind und wie sie eingesetzt werden
- Tipps und Tricks bei der Fehlersuche, wie Sie nachträglich die Störfestigkeit erhöhen können
- Ursachen, Auswirkungen und Abhilfen von statischer Entladung
- die Vor- und Nachteile unterschiedlicher Erdungsmethoden, welche Ursachen haben Potenzialdifferenzen, wie wird ein Potenzialausgleich durchgeführt
- Entstehung, Auswirkung, Vermeidung von Oberschwingungen, Netzresonanzen, Saugkreise, Sperrkreise etc.
- wie und wann werden Filter nutzbringend eingesetzt
- alles über Kabelschirm-Anbindungen
- Motorlagerströme, Entstehung, Auswirkung, Abhilfe
- die Aspekte des Blitzschutzes, vom Erkennen der Gefährdung bis zum Einsatz von Schutzelementen
- Einführung in die Normung, CE, Achtung neue EMV-Richtlinie!

Zielgruppe

Programmierer, Inbetriebsetzer, Projektierer, Servicepersonal, Instandhalter

Dauer

3 Tage

Teilnahmegebühr

Auf Anfrage

Kursort

Siehe Internet

Explosionsschutz Grundlagen (MP-EX-GRU)

Der Kurs vermittelt Herstellern und Verwendern elektrischer Betriebsmittel für explosionsgefährdete Bereiche das theoretische und praktische Basiswissen zum elektrischen Explosionsschutz. Hierzu gehören physikalische Grundlagen, Rechtsgrundlagen, mögliche Schutzmaßnahmen für elektrische Betriebsmittel und Hinweise zu Ihrer Anwendung. Durch Referat und Video-Filmausschnitte werden die Explosionszusammenhänge und -gefahren verdeutlicht.

Inhalte

- Explosion, Explosionsvoraussetzungen
- Zündquellen
- Primärer und sekundärer Explosionsschutz
- Sicherheitstechnische Kennzahlen
- Temperaturklassen, Explosionsgruppen, Zoneneinteilung
- Rechtsgrundlagen für den Explosionsschutz
- Zündschutzarten bei elektrischen Betriebsmitteln
- Baubestimmungen für Betriebsmittel nach EN 50 014-50 028
- Kennzeichnung elektrischer Betriebsmittel
- Anhand eines konkreten Betriebsmittels werden die speziell bei diesem Gerät realisierten Explosionsschutzmaßnahmen besprochen

Zielgruppe

Entscheider, Vertriebspersonal, Inbetriebsetzer, Projektierer, Servicepersonal, Instandhalter

Dauer

1 Tag

Teilnahmegebühr

Auf Anfrage

Kursort

Mannheim

Explosionsschutz Eigensicherheit (MP-EX-EIG)

Der Kurs vermittelt den Teilnehmern, die explosionsgeschützte elektrische Betriebsmittel und eigensichere Anlagen entwickeln, bauen bzw. betreuen, eine vertiefte Betrachtung der Zündschutzart, Eigensicherheit und den Aufbau von Betriebsmitteln mit eigensicheren Stromkreisen. Durch Anwendungsbeispiele wird der Einsatz eigensicherer Betriebsmittel erläutert. Außerdem wird der bei Zusammenschaltung von eigensicheren und zugehörigen Betriebsmitteln erforderliche Nachweis der Eigensicherheit anhand von Beispielen erläutert.

Inhalte

- Baubestimmungen für Betriebsmittel nach DIN EN 50 014 und 50 020
- Grundlagen der Zündschutzart, Eigensicherheit
- Zündgrenzkurven
- Eigensichere und zugehörige elektrische Betriebsmittel
- Eigenschaften spezieller eigensicherer Betriebsmittel, Kennzeichnung
- Anforderungen an das Errichten in den einzelnen Zonen nach DIN 0165
- Zusammenschaltung von Betriebsmitteln zu eigensicheren Anlagen/ Systemen (DIN EN 50 039)
- Errichtung eigensicherer Anlagen nach VDE 0165
- Betrieb, Instandsetzung, Prüfung von Betriebsmitteln

Zielgruppe

Entscheider, Vertriebspersonal, Inbetriebsetzer, Projektierer, Servicepersonal, Instandhalter

Dauer

1 Tag

Teilnahmegebühr

Auf Anfrage

Kursort

Mannheim

Aktuelle Termine, Kursorte und Preise entnehmen Sie bitte dem Internet unter der Adresse:

www.siemens.de/sitrain

11.5 Stichwortverzeichnis

Begriff	Seite
3-Klemmen-Konzept	8/24
4-Klemmen-Konzept	8/25
Abschaltgruppe	9/10
Aktoreinbindung am PROFIBUS	3/32
Aktoreinbindung mit ASIsafe	3/22
asimon	4/12
ASIsafe	3/19
ASIsafe Netze	4/12
ASIsafe Produktspektrum	5/20
Ausfallwahrscheinlichkeit	2/29
Auswerten	3/2
Automatik-Betrieb	8/3
baumustergeprüfte Sicherheitsfunktionen	8/3
Befehls- und Meldegeräte	5/8
Blanking-Funktionen	6/23
CNC-Steuerungen	8/2
CPU 315F	7/7
CPU 317F	7/7
CPU 414F	7/7
CPU 416F	7/7
CPU 417 H	7/7
Cross-Monitoring	8/3
Datensicherung, zusätzliche	4/5
Diagnosesoftware Auswertegeräte	6/21
Diagnosesoftware Lichtvorhänge	6/20
Drehzahl-/Stillstandsüberwachung	8/2, 8/9, 8/22
Ein-Kabel-Lösung	4/3
Einrichte-Betrieb	8/3
elektrische Sicherheit	1/10
EMV-Richtlinie	1/4
EnDat-Schnittstelle	8/5
Erfassen	3/2
ET 200S Safety Motorstarter Solution Local	5/26
ET 200S Safety Motorstarter Solution PROFIsafel	5/30
EU-Richtlinie	1/4
Europäische Maschinenrichtlinie	1/3, 1/5, 1/15, 1/20
Fertigungsautomatisierung	7/5
Frequenzsteuerung	9/6
Funktionale Sicherheit	1/2
Funktionsblock	2/17

Begriff	Seite
Gefahrbereichsabsicherung	6/3
gefahrbringender Ausfall	2/29
Grenzen einer Maschine	2/5
Gruppennormen	1/9
Hazard	2/5
Host-Guest-Kombination	6/20
IEC 62061	2/13
IM 151-7 CPU	7/7
Impulslöschung	8/11
ISO 13849 oder IEC 62061	2/15
Kategorien	1/15, 2/36
Kennung für Sender und Empfänger	4/5
Koexistenz	4/2
Konfigurationssoftware asimon	4/12
kontaktfreie Energietrennung	8/3, 8/9
konventionelle Sicherheitstechnik	7/4
Lebenszyklusmodell	2/2
Leistungsteil IPM25	9/8
Lichtgitter	6/17
Lichtvorhänge	6/16
Linearmotor	8/5, 8/6
MASTERDRIVES	9/2
Multi-Scan	6/22
Mutingfunktionen	6/25
Neutralleiter	1/19
Niederspannungsrichtlinie	1/15, 1/20
Normen	7/6
Not-Aus	1/9, 1/15
Not-Halt	8/11, 8/12, 8/14, 8/22, 8/25
Not-Halt Schalter	5/7
Nutztelegramme	4/4
P(lus)/M(asse)-schaltend	8/25, 8/26, 8/27, 8/28, 8/29
P(lus)/P(lus)-schaltend	8/26, 8/29
Positionsschalter	5/2
Powermodul PM-D F PROFIsafe	5/30, 9/10
Powermodul PM-D FX1	5/28, 9/11
prEN ISO 13849-1	2/12
Pressensteuergerät	5/14
Produktnormen	1/10

Begriff	Seite
PROFIBUS-Anbindung mit PROFIsafe	3/24
PROFIBUS-Nutzerorganisation	4/3
PROFIsafe-Profil	4/2
proprietäre Sicherheits-SPS	7/4
Prozessautomatisierung	7/5
Prozessleittechnik	1/21
Reagieren	3/2
Regelungsbaugruppe ICU24F	9/8
Restrisiko	1/12
Risikoabschätzung	2/6
Risikoanalyse	2/4
Risikobeurteilung	1/10, 2/6
Risikobewertung	2/6
Risikoelemente	2/9
Risikograph	2/12
Risikominderung	1/12, 2/3
Risikoreduzierung	1/22, 2/3, 2/6
Safety Integrity	2/9
Safety Performance	2/9
Safety-Matrix	7/10
Schutzfeldberechnung	6/9
Schutzleiter	1/19
Schutzumschaltung	6/6
Sensor-/Aktor-Einbindung	3/6
Sensoranbindung am PROFIBUS	3/25
Sensoranbindung an SIMATIC Modulen	3/25
Sensoranbindung mit ASIsafe	3/20
Sensorannbindung, Magnetschalter	3/28
Sensoreinbindung, konventionell	3/12
Seveso-Richtlinie	1/3, 1/20
Sicher reduzierte Geschwindigkeit (SG)	8/13, 9/9
Sichere Bremsrampe (SBR)	8/12, 9/8
Sichere Bremsenansteuerung (SBC)	9/5
Sichere programmierbare Logik (SPL)	8/14
Sichere Software-Nocken (SN)	8/13
Sicherer Betriebshalt (SBH)	8/12
Sicherer Halt (SH)	8/10, 9/3, 9/5, 9/8
sicherheitsbezogene Teile einer Steuerung	2/34
Sicherheitsgerichtete Ein-/Ausgangssignale (SGE/SGA)	8/15
Sicherheitsinformationen	4/4
Sicherheitsmonitor ASIsafe	4/10
sicherheitsrelevantes Steuerungssystem	2/19
Sicherheitsschaltgeräte	5/11
Sicherheitstelegramme, fortlaufende Nummerierung	4/5

Begriff	Seite
sicherheitstolerante Signale	4/2
SIL-Monitor	4/6
SIMATIC ET 200S	9/6
SIMODRIVE	8/8, 9/2
SINAMICS S120	9/4
SINUMERIK	8/8
Software-Endschalter (SE)	8/13
SRECS	2/19
Standardautomatisierung	7/3
Standort-Feld	4/2
Start, manuell	3/10
Start, überwacht	3/10
Starter	9/4, 9/6
Stillsetzen	1/16, 9/8
Stop-Kategorien	1/14
Stopreaktionen	8/9, 8/13, 8/22
Subsystem (Teilsystem)	2/18
Synchron-Einbaumotoren 1FE	8/6
Systemdesign	2/23
Systemdurchgriff	8/4
Systemintegration	2/26
Teilsystem (Subsystem)	2/18
Testbetrieb	8/31
Teststop	8/12, 8/28
Totmannbetrieb	8/31
Transceiver	6/19
Umformtechnik	8/32
Vektorregelung	9/6
Vorschriften	7/6
Wiederanlaufsperre	6/6
Zeiterwartung mit Quittierung	4/5

Impressum:

Safety Integrated:
Systemhandbuch Sicherheitstechnik, 5. Ausgabe

Herausgeber:
Siemens AG
Bereich Automatisierungs- und Antriebstechnik
Postfach 4848, D-90327 Erlangen

Für den Inhalt verantwortliche Autoren:
Georg Becker (A&D PT7)
Robert Gassner (A&D CD)
Maximilian Korff (A&D CD)
Hartmut von Krosigk (A&D ATS)
Jürgen Lange (A&D MC)
Stefan Lechner (A&D PT7)
Peter Maurer (A&D MC)
Guillaume Maigret (A&D CD)
Bernard Mysliwiec (A&D AS)
Uwe Schade (A&D CD)
Carsten Schmidt (A&D CD)
Jürgen Strässer (A&D MC)
Lutz Teschke (I&S IS)
Bernhard Wöll (A&D AS)

Konzept, Beratung, Koordination und Redaktion:
Wolfgang Kotitschke (A&D SE)
Johanna Gebhardt (A&D CD)
Sybill von Hofen (A&D GC)

Gestaltung:
NEW ORANGE DESIGN, Obernzenn

Druck:
Farbendruck Hofmann, Langenzenn

® 2005 by Siemens AG
Berlin und München

Alle Rechte vorbehalten
Schutzgebühr 20.- €

Wichtiger Hinweis:
Die hier beschriebenen Produkte wurden entwickelt, um als Teil einer Gesamtanlage oder Maschine sicherheitsgerichtete Funktionen zu übernehmen. Ein komplettes sicherheitsgerichtetes System enthält in der Regel Sensoren, Auswerteeinheiten, Meldegeräte und Konzepte für sichere Abschaltungen. Es liegt im Verantwortungsbereich des Herstellers einer Anlage oder Maschine, die korrekte Gesamtfunktion sicherzustellen. Die Siemens AG, seine Niederlassungen und Beteiligungsgesellschaften (im Folgenden „Siemens“) ist nicht in der Lage, alle Eigenschaften einer Gesamtanlage oder Maschine, die nicht durch Siemens konzipiert wurde, zu garantieren.

Siemens übernimmt auch keine Haftung für Empfehlungen, die durch dieses Handbuch gegeben bzw. impliziert werden. Für den korrekten und bestimmungsgemäßen Gebrauch der Produkte sind in jedem Fall die zugehörigen technischen Beschreibungen zu beachten.
Aufgrund dieses Handbuchs können keine neuen, über die allgemeinen Siemens-Lieferbedingungen hinausgehenden Garantie-, Gewährleistungs- oder Haftungsansprüche abgeleitet werden.

Änderungen vorbehalten

Siemens Aktiengesellschaft

Automation and Drives
Low Voltage Controls and Distribution
Postfach 3240, D-91050 Erlangen

Automation and Drives
Industrial Automation Systems
Postfach 4848, D-90327 Nürnberg

Automation and Drives
Motion Control Systems
Postfach 3180, D-91050 Erlangen

www.siemens.de/safety

Bestell-Nr. 6ZB5 000-0AA01-0BA1
Printed in Germany
Dispostelle 06 345 / SEK 30 296